AUDIT OF THE JUSTICE SECURITY OPERATIONS CENTER'S CAPABILITIES AND COORDINATION

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 11-46
September 2011

REDACTED – FOR PUBLIC RELEASE

AUDIT OF THE JUSTICE SECURITY OPERATIONS CENTER'S CAPABILITIES AND COORDINATION

EXECUTIVE SUMMARY*

Cyber security—the protection of information technology (IT) systems—presents an increasingly difficult challenge for the federal government in the defense of national interests. Weaknesses in information security policies and practices and the continually evolving nature of cyber threats imperil sensitive information from both internal and external sources. Protecting its own complex IT systems from intrusion remains a top management challenge for the Department of Justice (DOJ), which annually spends almost $3 billion on planning, implementing, and securing these systems. While DOJ has made significant progress in the area of IT security and has developed sound processes and procedures for identifying IT vulnerabilities, the need for effective strategies to track and mitigate computer system weaknesses remains.

To better meet this challenge, DOJ established the Justice Security Operations Center (JSOC) in 2007 to protect DOJ IT environments (systems, networks, and sensitive data) from cyber intrusions, incidents, attacks and espionage. JSOC mitigates threats and vulnerabilities by blocking known threats from accessing DOJ's systems and creating real-time alerts to components for immediate remediation as issues arise. JSOC provides incident response planning, training, and assistance to all DOJ components and works with components to prevent, monitor, mitigate, and resolve cyber incidents and attacks on DOJ. According to the Department of Commerce National Institute of Standards and Technology (NIST) Special Publication SP 800-94, Guide to Intrusion Detection and Prevention Systems, an incident is a violation or threat of violation of computer security, acceptable use, or standard security policy which may be caused by malicious means or accidentally.

JSOC also coordinates with the Department of Homeland Security (DHS), whose expanded role in cyber security oversight includes ongoing coordination with other federal agencies as well as state and local

---

* The full version of this report includes information that the Justice Management Division (JMD) and Federal Bureau of Investigation (FBI) considered to be law enforcement sensitive, and therefore cannot be publicly released. According to JMD and the FBI, disclosure of specific facility locations, network information, and specific software tools used would compromise DOJ's security. To create this public version of the report, the Office of the Inspector General redacted (blacked out) the portions of the full report that JMD and the FBI considered sensitive.

government officials, industry representatives, and international partners. Specifically, JSOC coordinates with the DHS's United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber incidents and attacks for the Executive Branch. Federal IT efforts also follow guidance issued by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and the Federal Information Security Management Act.[1]

OIG Audit Approach

The Office of the Inspector General (OIG) conducted this audit to assess JSOC's capabilities, and its cooperation and coordination with DOJ components and DHS's US-CERT efforts. The audit objectives were to assess: (1) JSOC's capabilities to prevent, identify, monitor, and respond to intrusion incidents; and (2) the effectiveness of the exchange of incident information and cooperation between JSOC and DOJ components.

We reviewed JSOC policies to evaluate incident response processes. We also interviewed officials from JSOC, various DOJ components and offices, US-CERT, and other federal agencies with Security Operation Centers (SOC). In addition, we tested samples of incident response tickets to determine JSOC's capabilities to monitor and respond to intrusion incidents and report to US-CERT. (JSOC uses the term "ticket" to refer to its electronic file for recording incident information.) Appendix I contains a more detailed description of our audit objectives, scope, and methodology.

Results in Brief

We assessed JSOC's effectiveness in terms of the resources, policies, and procedures it uses to respond to and report incidents within DOJ and to US-CERT, as well as how it communicates its services to and coordinates with the components. We found that JSOC has many processes and procedures that appear to provide effective network monitoring, reports incidents to US-CERT, and coordinates with DOJ components. In general, JSOC's policies and procedures follow guidance issued by US-CERT and other federal oversight agencies. JSOC has made efforts to reduce the length of time incident tickets remain open by adding the "Closer" role and emphasizing that components and JSOC analysts follow established processes. Components are also generally satisfied with their interactions

[1] The Federal Information Security Management Act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

with JSOC and the support it offers, although some components were not always aware of JSOC's services.

However, we also believe improvements can be made to provide additional incident monitoring capabilities and component coordination, such as improved incident ticket processes, more comprehensive policies and updates, and additional support for integrating component processes with JSOC. Specifically, we believe JSOC should conduct risk assessments to determine timeframes for opening and closing tickets, and further define and document these processes to mitigate the potential cyber security risk.

In our testing of incident tickets over two sample periods, we found that JSOC allows additional time for reporting incidents than what US-CERT advises.[2] We also found that some incident tickets lack sufficient documentation for adequate monitoring and closure and some remain open for an extended time. In addition, because JSOC did not explicitly define widespread incidents and did not have an auditable process in place for tracking these incidents, we could not determine if infected resources are accurately identified, reported, and monitored.

While most components and offices provide JSOC with required information feeds from their internal networks, six components have not provided all available information feeds, therefore limiting the efficiency of JSOC to monitor cyber activity and conduct event correlation, or determine whether there are any relationships among this activity.[3] Our review also found that the FBI's process is to not report to JSOC incidents it categorizes as under investigation, which prevents JSOC from having a comprehensive view of the network. In addition, we found that JSOC is unable to monitor traffic from some components' external connections, potentially increasing DOJ network exposure to intrusion or attack.

---

[2] We initially sampled 533 out of 1,996 incident tickets that were open between January 4 and June 24, 2010. To account for actions taken by JSOC during our audit to improve monitoring and response capabilities, we sampled an additional 133 out of 512 incident tickets that were open between September 20 and October 22, 2010.

[3] An information feed is a direct, real-time or near real-time electronic data input of relevant security monitoring and auditing data. Component activity is submitted and monitored on four network feeds that allow JSOC to correlate information on events to monitor for malicious attacks. Event correlation examines the relationship among events across an IT infrastructure to narrow the search for the cause of a problem. The six components that have not provided all information feeds are the Civil Division, Executive Office for United States Attorneys, Federal Bureau of Investigation, Office of Inspector General, United States Marshals Service, and United States Parole Commission.

In our report, we make 20 recommendations to improve JSOC's capabilities to report and manage information on cyber incidents and enhance the effectiveness of coordination between JSOC and DOJ components and offices.

Our report contains detailed information on the full results of our review of JSOC. The remaining sections of this Executive Summary provide more detail on our audit findings.

JSOC's Incident Reporting Responsibilities and Capabilities

While JSOC appears to generally be performing effectively in its incident monitoring capabilities, the audit identified some weaknesses in JSOC's operations. Specifically, these pertain to JSOC's incident reporting requirements, including questionable timeframes for opening incident tickets; lack of timeframes for closing incident tickets; a failure to consistently document incidents; and a lack of an auditable process for tracking widespread incidents. We also found that several of JSOC's policies regarding incident response processes are not finalized, are ambiguous, or do not reflect current operations.

Data loss and malicious code represent the two most frequent types of incidents reported by components to JSOC. Data loss occurs when individuals suffer a loss of any sensitive data or data-containing devices such as laptops, BlackBerry devices, USB thumb drives, or physical papers. Examples of malicious code or software campaigns include denial-of-service attacks or attempts by attackers to trick users into downloading malicious software.[4] Computer users can be tricked into accessing malicious links in social networking posts; through Internet searches by users related to significant events, such as the Mississippi flood disaster or Osama bin Laden's death, that lead to websites with malicious content; and in prompts, or links, that appear in e-mail messages or when visiting websites that direct the user to download certain content, such as videos.

Our analysis identified concerns regarding excessive timeframes for opening and closing incident tickets in Remedy, the software used by JSOC to track and manage reported cyber incidents within DOJ. While US-CERT provides timeframes for incident reporting that range from 1 hour to 30 days depending on the incident category, JSOC's interpretation of US-CERT's guidelines allows JSOC up to twice as much time to report incidents to

[4] A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

US-CERT. For example, US-CERT indicates that an unauthorized access incident should be reported within 1 hour of detection. JSOC's interpretation allows 1 hour for an unauthorized access incident to be reported by a component to JSOC, then 1 additional hour for JSOC to report the incident to US-CERT. However, we were told that JSOC requests its analysts to report incidents to US-CERT upon receipt.

We also found that JSOC lacks guidance regarding the amount of time it should take to resolve incident tickets, which allows some to remain open for an extended period of time, including up to several months. For example, we found that for incidents categorized as data loss, 10 percent of the tickets sampled in our original population and 6 percent of the tickets sampled from a subsequent population were open longer than 30 days. The longer a US-CERT-reportable ticket remains unresolved—and therefore a vulnerability may exist—the computer system remains at risk for potential malicious actions, such as the spread of malware, or software programs designed to damage or perform unwanted actions.[5] During our review, JSOC added a reviewer role designated as the "Closer," or person responsible for reviewing tickets aged over 30 days.[6] JSOC officials believe this new review role will result in more timely resolution of incident tickets.

In addition to our testing of individual incident tickets, we also looked at JSOC's procedures for reporting and tracking related incidents. We found that JSOC did not explicitly define widespread incidents and did not have an auditable process in place for tracking these incidents and their impact. While we found that JSOC management tracked widespread incidents on an ad-hoc basis, this approach is not clearly defined, does not allow for clear measurement or assessment of performance, and may not account for all such incidents or their effects.

We also found that JSOC's policies regarding incident response include potentially conflicting processes or lack up-to-date information regarding appropriate incident response actions. This may result in increased risk within DOJ's incident management process if staff are not following current and proper procedures to document and respond to incidents.

---

[5] A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[6] According to JSOC, the Closer responsibility is an additional task assigned to JSOC staff as needed, not a new staff position.

JSOC Coordination with Components

JSOC policy requires components to report incidents to JSOC. The audit identified several weaknesses regarding coordination between components and JSOC. For example, we found that six components have not provided JSOC with all available information feeds for JSOC to monitor and conduct event correlation. Event correlation examines the relationship among events across an IT infrastructure to narrow the search for the cause of a problem. Additionally, some components maintain external Internet connections separate from DOJ's Trusted Internet Connection (TIC)—its main Internet access point.[7] Thus, JSOC is unable to monitor traffic from these external connections, potentially increasing DOJ network exposure to intrusion or attack.

During our interviews with 13 components and offices, we learned that at least 2 components were unaware of some JSOC capabilities. For example, these components were not aware of the forensic services that JSOC provides, such as performing an evaluation of a hard drive that had been compromised by a virus or for an internal investigation. Limited awareness reduces component ability to take advantage of services provided to enhance the protection of the DOJ network.

Additionally, the FBI's process of not reporting to JSOC incidents it categorizes as under investigation does not comply with the Office of Chief Information Officer (OCIO)–authorized and distributed DOJ Computer System Incident Response Plan.[8] This may limit JSOC's awareness of IT security risks to the FBI and DOJ, and prolongs the potential vulnerability of the network since JSOC is unable to offer guidance regarding these incidents or seek advice from US-CERT. Although the FBI maintains a separate Security Operations Center, known as ESOC, as discussed below, JSOC is responsible for reporting all DOJ incidents to US-CERT.

---

[7] The Trusted Internet Connection initiative was mandated by the Office of Management and Budget Memorandum 08-05, Implementation of Trusted Internet Connections, issued in November 2007. Among other things, the initiative was intended to improve the federal government's incident response capability by reducing the number of external Internet access points and centralizing gateway monitoring. In DOJ, the TIC allows JSOC to monitor a single flow of network traffic.

[8] The FBI informed the audit team in a meeting that it has provided a small number of incidents categorized under investigation to JSOC. However, since the FBI's process is to not report incidents categorized under investigation because it believes it is under no requirement to do so, this brings into question whether sufficient information is being provided to JSOC in a timely manner, based on the periodic reporting requirement stated in the DOJ Computer System Incident Response Plan.

JSOC and US-CERT Interaction

In addition to coordinating with components on incident reporting, JSOC is responsible for alerting US-CERT of incidents within US-CERT-reportable categories that occur at DOJ. The audit did not identify any issues regarding JSOC's reporting to US-CERT in accordance with US-CERT guidance. While US-CERT officials informed us that they were not aware of any reporting issues concerning the timeliness or comprehensiveness of JSOC-reported information, US-CERT is only aware of timeframes based on information provided by JSOC. US-CERT officials said that it only provides reporting guidelines and has no formal authority to enforce reporting requirements.[9] Thus, US-CERT depends on DOJ and other agencies to follow other federal information security requirements and develop internal processes for conducting IT environment risk assessments and managing incident detection to meet US-CERT reporting guidance. US-CERT's role is to primarily support information sharing and collaboration among reporting entities regarding cyber security.

Conclusion and Recommendations

In general, JSOC has processes and procedures that appear to provide effective monitoring on network traffic and information it receives from DOJ components and offices. JSOC also provides incident response training to and coordinates with DOJ components and reports to US-CERT. However, based on our analysis, we believe improvements can be made to provide additional incident monitoring capabilities and component coordination, such as improved incident ticket processes, more comprehensive policies and updates, and additional support for integrating component processes with JSOC. We recognize JSOC's efforts to reduce the length of time tickets remain open by adding the "Closer" role and emphasizing that components and JSOC analysts follow established processes. However, we believe JSOC should pursue additional efforts, such as conducting risk assessments to determine timeframes for opening and closing tickets, and further define and document these processes to mitigate the potential cyber security risk.

---

[9] Richard L. Skinner, Inspector General, U. S. Department of Homeland Security, before the Committee on Homeland Security, U.S. House of Representatives, concerning "U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain" (June 16, 2010), http://www.dhs.gov/xoig/assets/testimony/OIGtm_RLS_061610.pdf (accessed April 25, 2011) noted that US-CERT does not have enforcement authority to address security incidents.

During our review of JSOC's coordination with components, we found that six components have yet to provide JSOC with all available information to enable effective and efficient network monitoring and event correlation. We also identified that at least 2 out of 13 components and offices were not fully aware of all JSOC's services, limiting their ability to take advantage of all that JSOC offers. Our review also found that the FBI's process of not reporting to JSOC incidents that it categorizes as under investigation may prevent JSOC from having a comprehensive view of the network, potentially allowing US-CERT-reportable incidents to remain uncategorized and allowing the IT environment to remain vulnerable for an extended period of time.

Our audit work and findings resulted in 20 recommendations to assist JCOC in responding to and reporting incidents within DOJ and to US-CERT, as well as enhance JSOC's coordination with the components. For example, we recommend that JSOC develop additional guidance regarding ticket monitoring including documenting on a weekly basis its oversight of open incident tickets in Remedy, including those in reportable categories as well as those under investigation. We also recommend that JSOC improve its documentation efforts for initial classification of incidents, follow-up, and resolution. In addition, JSOC should ensure that it obtains information feeds and incident reports from all DOJ components to adequately monitor networks and respond to incidents, including incidents categorized as under investigation by the FBI.

AUDIT OF THE JUSTICE SECURITY OPERATIONS CENTER'S CAPABILITIES AND COORDINATION

TABLE OF CONTENTS

INTRODUCTION

Background

Established in August 2007, JSOC is responsible for providing leadership and guidance to all DOJ components in the areas of incident response (IR), including IR planning and establishing a DOJ-wide incident response environment that facilitates cooperation with components responsible for handling security incidents that affect DOJ. JSOC is responsible for network security which includes monitoring DOJ's primary Internet access point and component traffic. JSOC assists components with the reporting, monitoring, and resolution of their incidents, and acts as the main reporting source to US-CERT based on US-CERT's guidelines. In addition to its US-CERT obligations, JSOC assumed the prior IT security functions of the DOJ Computer Emergency Readiness Team, which directed federal agencies to establish procedures for detecting, reporting, and responding to security incidents. DOJ components have a responsibility to inform JSOC of incidents that are reportable, according to a specific requirement in the DOJ Computer System Incident Response Plan.

US-CERT was established in 2003 as a partnership between the Department of Homeland Security and the public and private sectors, for the purpose of coordinating the response to security threats from the Internet. As the operational arm of DHS's National Cyber Security Division, US-CERT provides response support and defense against cyber attacks for the federal civilian sector and shares information with state and local government officials, industry representatives, and international partners. Through US-CERT's coordination with these entities it collects and disseminates cyber security information to the public. US-CERT issues both non-technical and technical documents from topics such as "Securing Your Computer" and "General Internet Security" to "Computer Forensics" and the "National Strategy to Secure Cyberspace". US-CERT also issues monthly and quarterly activity reports documenting high-impact security threats and vulnerabilities reported to it. These reports, obtainable through US-CERT's website, also contain various cyber security alerts, cyber security tips, and resource and contact information.

To perform its role, US-CERT acquires reporting data from federal agencies in five incident categories, as shown in Exhibit 1. Two other categories—Category 0, Exercise/Network Defense Testing and Category 6, Investigation—do not require reporting to US-CERT. Rather, these are for each agency's internal use.

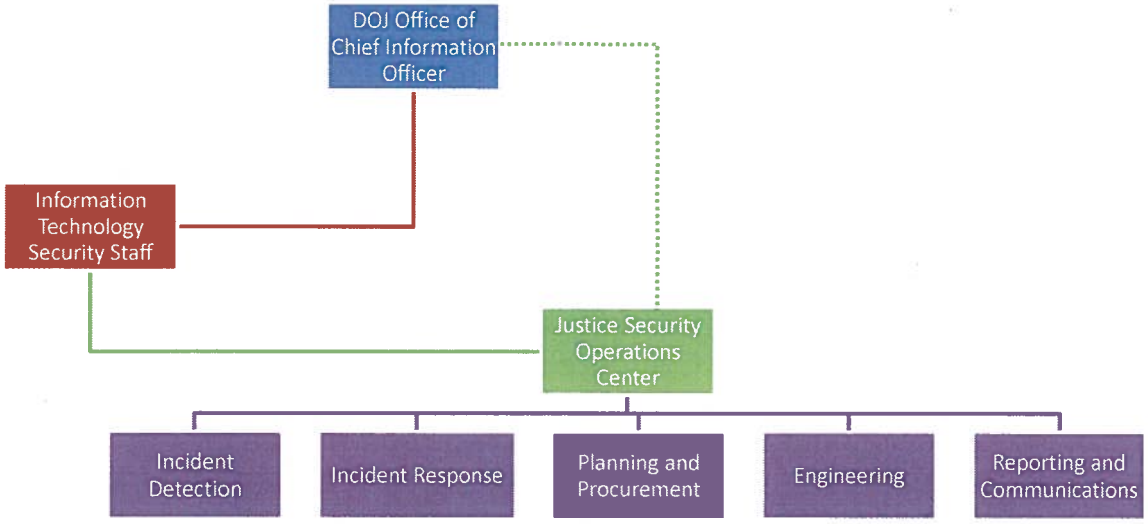
EXHIBIT 1: FEDERAL AGENCY INCIDENT CATEGORIES AS DEFINED BY US-CERT

	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

**Defined by NIST Special Publication* 800-61
Source: US-CERT, "Federal Incident Reporting Guidelines," http://www.us-cert.gov/federal/reportingRequirements.html (accessed April 21, 2011).

In addition to these categories, JSOC created Category 8 (Data Loss), as a sub-category of Category 1 (Unauthorized Access), for internal incident tracking purposes. JSOC reports Category 8 incidents to US-CERT under

EXHIBIT 2: JSOC ORGANIZATIONAL CHART



Source: JSOC

[redacted][11][redacted][12][redacted]

Through incident notification, monitoring, and reporting, JSOC's goal is to prevent, detect, and respond to cyber threats against DOJ and its components. Components can contact JSOC by e-mail or phone, or submit incidents under investigation through the Remedy electronic system to obtain feedback from JSOC analysts. (The next section describes the

[11] [redacted]

[12] [redacted]

Category 1. JSOC also uses Category 6 to track potential incidents under investigation, which are not required to be reported to US-CERT. Additionally, JSOC created Category 7 (Spam) and tracks these occurrences internally.

While US-CERT criteria specify when incidents in each category should be reported, JSOC formally requires its analysts to report each incident upon identification of reportable category, regardless of category timeframes. JSOC also informally requests components to do the same.

In addition to its US-CERT obligations, JSOC assumed the prior IT security functions of the DOJ Computer Emergency Readiness Team (DOJCERT). DOJCERT was created in 2000 in response to the Government Information Security Reform Act and directed federal agencies to establish procedures for detecting, reporting, and responding to security incidents. As mentioned previously, DOJ components have a responsibility to inform JSOC of incidents that are reportable according to a DOJ requirement.[10] JSOC, in turn, is responsible for network security, including assisting components with the reporting, monitoring, and resolution of their incidents, and acts as the main reporting source to US-CERT based on US-CERT's guidelines.

JSOC Organization and Responsibilities

JSOC incident response staff support components with training and guidance, while also providing oversight and coordinating DOJ-wide incident response actions. JSOC reports to both the IT Security Staff and to the DOJ Chief Information Officer, as shown in Exhibit 2.

[10] DOJ Computer System Incident Response Plan

various features of and how JSOC uses the Remedy system.) JSOC also communicates security awareness information to components through e-mail advisories generated internally or as received from US-CERT. JSOC provides training for the components in the areas of information security and incident response. In addition, JSOC participates in internal working groups, such as the DOJ Office of Chief Information Officer working group, and DOJ's annual Cyber Security Conference. JSOC officials also meet regularly with other federal IT security offices to exchange information regarding current security threats.

Given its primary oversight role for unclassified DOJ systems, JSOC is responsible for monitoring and securing the Trusted Internet Connection (TIC), or the primary Internet entry point for the DOJ, and reviewing all DOJ traffic that enters through the TIC.[13] All components, with the exception of the FBI, use the DOJ TIC.[14] We found that, on an as-needed basis, some special DOJ programs need Internet access outside the TIC, such as Internet connections established for investigation purposes. These lines protect DOJ's identity during law enforcement investigations or from exposure to malware in IT investigations. Notwithstanding these special lines, as of January 2011, several internet connections outside the DOJ TIC were being actively assessed and integrated into the DOJ TIC by components to achieve full compliance as part of the government-wide TIC initiative to consolidate Internet access points.

While it mainly conducts unclassified monitoring, JSOC provides limited monitoring of classified systems within the TIC as requested. To allow for increased processing of classified information along with its monitoring of unclassified activity, in October 2010, JSOC migrated all of its operations into a sensitive compartmented information facility (SCIF).[15] In addition,

---

[13] The Trusted Internet Connection (TIC) initiative was mandated by the Office of Management and Budget Memorandum 08-05, Implementation of Trusted Internet Connections, issued in November 2007. Among other things, the initiative was intended to improve the federal government's incident response capability by reducing the number of external Internet access points and centralizing gateway monitoring. Within DOJ, the TIC allows JSOC to monitor a single flow of network traffic. DOJ maintains a primary and an alternate TIC that for the purpose of this audit are considered to be one TIC.

[14] [redacted]

[15] A sensitive compartmented information facility (SCIF) is an accredited area used for classified processing.

JSOC relies on the components to manage their own classified networks, to provide JSOC with unclassified sensitive information when issues arise on their networks, such as data spills.[16]

JSOC Incident Response Capabilities

Incidents can be identified by components' internal monitoring, by JSOC through its TIC oversight, or from component information feeds received by JSOC. For each identified incident, JSOC analysts open, or create, an incident ticket in Remedy, which stores data on cyber incidents within DOJ and tracks JSOC's internal monitoring. JSOC or component staff categorize incidents based on their investigation of and the characteristics that an incident exhibits.[17] Once JSOC opens an incident ticket, it also reports the incident in US-CERT's Remedy portal. JSOC analysts also notify the appropriate IR contacts at the components and JSOC management as needed. JSOC staff are responsible for monitoring incidents until tickets are closed.

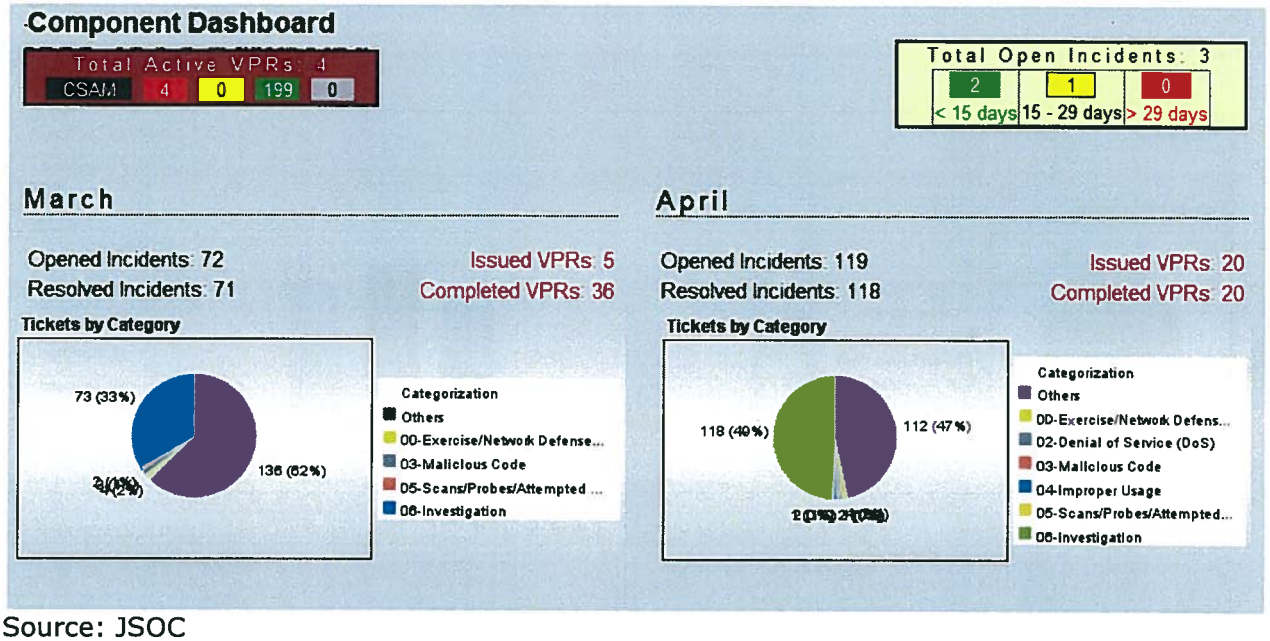
Incident tickets collect information such as organization type, incident status, description, date, and resources affected. Remedy's incident ticketing system features a dashboard that displays updated ticket summary information, such as ticket age and number of open tickets. The dashboard provides real-time statistics for components regarding the status of their tickets, including information on US-CERT reportable categories, as shown in Exhibit 3. The dashboard also indicates how long incidents have been in "open" status by using a color-coded ticket aging system—identifying open tickets 1-15 days old as green, 15-29 days old as yellow, and more than 29 days old as red. The dashboard allows a component to view only information specific to that component.

In the dashboard example below, JSOC can compare a component's incident activity for March and April, including the numbers of incidents opened, incidents resolved, and the number of incidents per category.

[16] A data spill is a security incident that results in the transfer of sensitive information to an unauthorized system.

[17] [redacted]

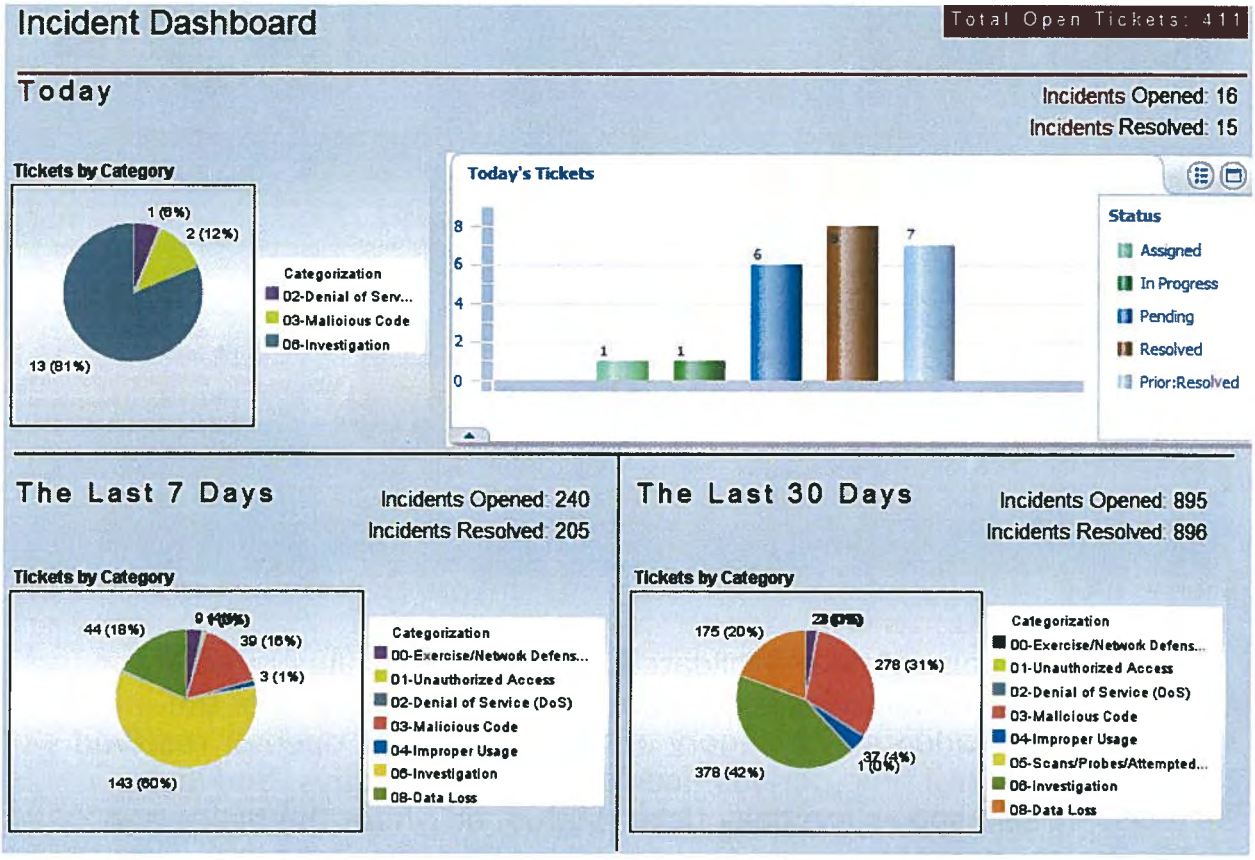
EXHIBIT 3: EXAMPLE OF JSOC'S COMPONENT DASHBOARD



Source: JSOC

JSOC can also view consolidated information, as illustrated in Exhibit 4. This consolidated dashboard provides a snapshot of the breakdown of incidents by category and the number of open or resolved tickets over several time periods—current day, last 7 days, and last 30 days. It also shows the daily ticket status, or where the ticket is in JSOC's review process.

EXHIBIT 4: EXAMPLE OF JSOC'S CONSOLIDATED INCIDENT DASHBOARD



Source: JSOC

[redacted]

[redacted]

[redacted]

JSOC employs other specialty software to perform threat analysis. NetWitness, for example, is a program that allows JSOC to analyze network traffic between DOJ's internal network and the Internet to provide network-based forensics. Using NetWitness, a JSOC analyst can reconstruct raw network data to analyze threats. Additionally, data in NetWitness automatically feeds into [redacted] for live monitoring purposes. Each feed provides more detail to events that allows for correlation to monitor for incidents.

JSOC also performs host-based forensics, which allows JSOC to analyze potentially compromised systems to determine the method of exploitation, recover attacker tools, and assess potential data loss. Forensic services are available to DOJ components if the need arises based on incidents. JSOC performs forensic work with tools such as [redacted], a computer forensic software used to analyze digital media. Additional software such as Wireshark, an open-source packet analyzer, is used to perform further forensic work at the network level.

Component Incident Response Capabilities

JSOC relies on components' and offices' Security Operations Centers (SOC) and Incident Response (IR) teams to communicate any incidents detected to JSOC. We selected 13 components and offices for review. Our sample included all four SOCs and nine variably sized components or offices with IR teams. We found that for the 13 components and offices we reviewed, the level of reliance on JSOC varies depending on the capability of their SOCs or IR teams. Both the FBI and the Executive Office for United States Attorneys have mature SOCs based on experience, level of operational development, additional monitoring capabilities (including 24/7 schedules), and dedicated staffing.

[redacted]

[redacted][19]

Security Operations Policies and Procedures

We identified limited federal guidance pertaining specifically to SOC operations. Federal government publications provide some guidance related to responsibilities SOCs have, including incident response, rather than directly state how a SOC should function. For example, the National Institute of Standards and Technology's (NIST) Special Publication 800-61 Computer Security Incident Handling Guide, provides guidance for incident response teams, acknowledges the requirements for federal agencies to report to US-CERT and establish a primary point of contact, and provides guidance on incident response capabilities and communications responsibilities.[20] Other NIST policies provide guidance on processes for malware analysis, forensic analysis, security log management, intrusion detection, and prevention systems, all of which JSOC performs.[21]

We reviewed 22 JSOC policies and procedures that JSOC provided us regarding incident response, including its Incident Reporting Handbook and various standard operating procedures (SOP) specific to operations and communication.[22] Our review found that JSOC's policies provide direction on multiple elements of incident detection throughout DOJ. For example, JSOC's SOPs include information on using specific applications such as [redacted] and Remedy, roles and responsibilities of specific teams, and interactions specific to a component. We also found that some federal

[19] [redacted]

[20] NIST SP 800-61 Rev. 1, Computer Security Incident Handling Guide, (March 2008).

[21] NIST SP 800-83, Guide to Malware Incident Prevention and Handling (November 2005); NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response (August 2006); NIST SP 800-92 Guide to Computer Security Log Management (September 2006), and NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (February 2007).

[22] The list of JSOC-provided policies and procedures we reviewed can be found in Appendix III.

agencies consider JSOC policies for guidance when implementing policy within their own SOCs.

Prior Related Reviews

In June 2007, the OIG issued a review of the DOJ's reporting procedures for the loss of sensitive electronic information.[23] The purpose of this review was to provide an overview of the policies and procedures that DOJ components were required to follow to respond to and report computer security incidents. This report reviewed DOJCERT (JSOC's predecessor organization) and nine components' policies and procedures regarding reporting and identifying losses of sensitive information, including personally identifiable information (PII), classified information, and notification of affected parties of losses of their sensitive information. The report provided eight recommendations to help the DOJ improve its computer security incident reporting procedures, including developing a department-specific definition of PII and raising awareness within the components regarding incident reporting requirements. As of September 2010, the DOJ completed corrective actions on all eight recommendations and as a result, the OIG closed the report.

In September 2009, the DHS issued a report on DOJ's TIC Compliance Validation, an assessment used to measure compliance with the Federal TIC Initiative to consolidate Internet access points within each agency.[24] This report stressed the need for DOJ to improve its technical capabilities as a single-service Trusted Internet Connection Access Provider. DOJ is working to resolve issues identified in the report, including the completion of JSOC's migration into a 24/7 operation and continued efforts to bring in multiple external Internet access points into the TIC.

In March 2010, GAO published a report on the status of federal agencies' efforts to respond to the Trusted Internet Connection initiative and the National Cybersecurity Protection System.[25] GAO reported that as of September 2009, none of the 23 major executive branch agencies had met

---

[23] U.S. Department of Justice Office of Inspector General, *Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information*, Evaluation and Inspection Report, I-2007-005 (June 2007).

[24] U.S. Department of Homeland Security, *Trusted Internet Connection Initiative, Department of Homeland Security TIC Compliance Validation Report*, (September 2009).

[25] U.S. Government Accountability Office, Information *Security – Concerted Effort Needed to Reduce and Secure Internet Connections at Federal Agencies*, GAO-10-237 (March 2010).

all of the requirements of the Federal TIC Initiative. Additionally, while most agencies reported making progress toward reducing their external connections and implementing critical security capabilities, they have also experienced delays in implementation efforts due to logistic and external agreement issues.

FINDINGS AND RECOMMENDATIONS

I. JSOC Efforts to Monitor Components' Incident Response and Comply with US-CERT Guidelines

To assess the effectiveness of JSOC's incident response capabilities, we analyzed two samples of incident reports in JSOC's Remedy ticket system as well as examined JSOC's operational policies. We identified weaknesses in both JSOC's response to incidents and in its operational capabilities.

Specifically, we found that: (1) timeframes for opening and closing tickets in Remedy are excessive, resulting in potential delays in the reporting and resolution of incidents; (2) incident tickets do not include sufficient documentation to ensure appropriate monitoring responsibility and closure; and (3) widespread incidents are not tracked using an auditable process, which may result in inaccurate identification, reporting, and monitoring of infected resources. We also determined that some JSOC policies do not reflect current operations and thus allow inconsistent performance that can cause delays or inaccuracies in monitoring and reporting.

JSOC Requirements for Reporting Incidents

We reviewed JSOC's policies and interviewed JSOC management to understand JSOC's capabilities and operations as these relate to how it detects, monitors, and tracks cyber incidents. JSOC has 15 standard operating procedures that provide detail on specific processes, such as for Remedy or JSOC communications, and an incident handbook that discusses incident reporting procedures. Generally, we found JSOC policies provide sufficient technical detail on how security analysts should implement the incident reporting process. However, we are concerned about the excessive timeframes for both opening and resolving tickets in Remedy based on JSOC policies.

Timeframe for Opening Tickets

We interviewed JSOC officials regarding the timeframe for reporting incident tickets to US-CERT based on when incidents are detected, as described in US-CERT's guidance in Exhibit 1. JSOC officials informed us that they have an informal agreement with US-CERT that the detection date is when JSOC receives a categorized incident notification from the component rather than the time the incident may have been detected at the

component. However, when we interviewed US-CERT officials, we were informed that no such agreement existed. US-CERT officials informed us that a risk assessment should be performed by the agency to determine the initial timeframe for reporting an incident, since no defined requirements exist and US-CERT does not actively track an agency's timeliness. JSOC officials were unable to provide us with documentation on risk assessment to help explain how the timeframe for reporting is initiated. However, we found that both JSOC's Incident Reporting Handbook and DOJ's Computer System Incident Response Plan identify timeframes for reporting incidents using US-CERT's guidance.

As shown in Exhibit 1, US-CERT provides incident reporting timeframe criteria to agencies that varies depending upon the incident category. For example, a Category 1 (Unauthorized Access) incident should be reported to US-CERT within 1 hour of discovery or detection. JSOC considers its reporting process to US-CERT to begin when an incident is determined as a reportable category and communicated to JSOC. Given a Category 1 incident, JSOC would allow a component 1 hour to report the incident to JSOC, then JSOC would have 1 hour to report the incident to US-CERT. However, JSOC officials told us they also informally advise components to report incidents as soon as possible. Strictly applied, US-CERT's reporting guidance begins at the time an incident is first detected at a component and determined to be a reportable category and ends when the incident is reported to US-CERT.[26] Allowing twice the required time to report an incident to US-CERT may potentially increase opportunities for malicious actions within DOJ and add to the overall risk to its IT environment.

Incident tickets initially opened in Category 6 (Investigation) are not required to be reported to US-CERT until they are reclassified into a reportable category. The time of reclassification would be considered as the incident detection time.

We discussed our concern with JSOC officials regarding the excessive amount of time that may be allowed from the actual detection date of an incident within a component to the reporting date to US-CERT. Although JSOC officials informed us that JSOC provides informal guidance to components to report immediately to JSOC when an incident occurs, this

---

[26] Our analysis assumed that upon incident detection, the component either places the incident into a reportable category immediately or places the incident into Category 6 (Investigation). Based on US-CERT reporting guidelines, Category 6 is not reportable. A Category 6 ticket will eventually be reclassified after further investigation as either a non-issue or a reportable category. Subsequently, we used either the time of detection or the time the ticket was placed into a reportable category for our analysis.

guidance is not documented. JSOC officials also told us that JSOC analysts are expected to report the opening of incident tickets to US-CERT immediately upon their classification into one of the US-CERT reportable categories.

Based on our review of how and when tickets are opened, we did not find any justification for a component to need the entire timeframe JSOC allots to report an incident. We believe that adherence to US-CERT reporting guidelines should apply from when an incident is identified, rather than granting both a component and JSOC the same amount of time to report the incident to US-CERT. However, if the results of an internal risk assessment warrant additional time or different reporting requirements, JSOC should document the justification for modifying its reporting requirements to meet US-CERT guidelines. Without a risk assessment to determine guidelines for the timeframe for incident reporting, we cannot determine whether JSOC's policy of allowing components the full US-CERT reporting timeframe has thoroughly considered the potential risk or effect that may result from its extended reporting times. At a minimum, JSOC's interpretation of US-CERT's reporting timeframe may potentially increase the vulnerability of DOJ's IT environment by delaying action to resolve issues.[27]

Timeframe for Ticket Resolution

We interviewed JSOC officials and reviewed policies and found that there was no policy indicating a required timeframe for a ticket to be resolved. A resolved ticket is an incident that has been closed by a JSOC analyst because it no longer represents a risk. The decision to resolve the ticket is made based on communications with the individual at the component managing the closure of the incident. An unresolved ticket poses a potential risk to the network. While JSOC does not have guidance regarding appropriate or expected timeframes for resolving incidents, it does monitor the aging of an incident ticket, coding tickets over 30 days as red and in need of additional feedback. As explained below, we found that JSOC had a high population of aged tickets.

We initially reviewed 1,912 incident tickets in Remedy from January 4, 2010, through June 24, 2010, to assess the timeliness with which these

[27] A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

incidents were resolved, or ready to be closed.[28] We found that tickets did not appear to be resolved timely, with many tickets open for an extended period of time, exceeding 30 days.

During our review, JSOC reinforced its processes to improve its ticket resolution process and added a reviewer role designated as the "Closer," or person responsible for reviewing tickets aged over 30 days.[29] JSOC officials believe this new review role will result in more timely resolution of incident tickets. To account for the improvements that JSOC made during our audit, we reviewed an additional 402 tickets in Remedy that were resolved from September 20, 2010, through October 22, 2010.[30] While most of the tickets in both populations were resolved within 10 days, risk remains for tickets left unresolved for an extended period of time. As shown in Exhibit 5, the average age of a ticket and the percentage of tickets open for longer than 30 days decreased by 4 percent once JSOC made improvements in its processes. However, 25 incident tickets still exceeded 30 days.

EXHIBIT 5: AGE OF RESOLVED INCIDENT TICKETS

	Original Population		**Second Population**	
Total ticket population	1,912		402	
Average Age	8.55 days		6.40 days	
Ticket Age	*Number*	*Percentage*	*Number*	*Percentage*
0-10 days	1,565	82%	341	85%
10-20 days	92	5%	17	4%
20-30 days	62	3%	19	5%
> 30 days	193	10%	25	6%

Source: OIG assessment of JSOC-provided Remedy tickets

We also found that with tickets involving data loss incidents (Category 8), the responsibility for investigating and handling the incident falls primarily on the component rather than JSOC, which makes it more difficult for JSOC to monitor the resolution of these incident tickets. JSOC's ability to monitor Category 8 tickets (involving data loss) is generally limited because it primarily relies on monitoring by the affected component, which

[28] We reviewed only tickets that had reached a resolved status, indicating they were ready for closure. Consequently, the number we reviewed is less than the entire population of tickets open during that time period (1,996 tickets) because some tickets remained unresolved.

[29] According to JSOC, the Closer responsibility is an additional task assigned to JSOC staff as needed, not a new staff position.

[30] The entire population of open tickets during this time period was 512.

may lead to longer timeframes for resolving incidents. However, when comparing aging data for tickets excluding Category 8, as shown in Exhibit 6, with aging data including Category 8 tickets, we found the latter showed a reduction in the overall average age of an incident ticket, as shown in Exhibit 5.

EXHIBIT 6: AGE OF RESOLVED INCIDENT TICKETS, EXCLUDING CATEGORY 8 (DATA LOSS) TICKETS

	Original Population		Second Population	
Total Ticket Population	1,110		292	
Average Age	12.74 days		8.40 days	
Ticket Age	*Number*	*Percentage*	*Number*	*Percentage*
0-10 days	809	73%	234	80%
10-20 days	67	6%	16	5%
20-30 days	57	5%	17	6%
> 30 days	177	16%	25	9%

Source: OIG assessment of JSOC-provided Remedy tickets

We then reviewed the tickets in these populations according to their reporting categories to determine the average time for resolving incidents based on the incident type. Exhibit 7 illustrates the average time to resolve incidents in categories 1, 2, 3, 4, 5, and 8. Tickets in Category 6, or incidents under investigation, are not resolved in this category. Instead, these incidents are eventually reclassified to another category for reporting purposes.

EXHIBIT 7: AVERAGE AGE OF RESOLVED INCIDENT TICKETS BY CATEGORY

Ticket Category	Original Population		Second Population	
	Average Days	*# of tickets*	*Average Days*	*# of tickets*
1 – Unauthorized Access	47.24	6	0.16	1
2 – Denial of Service	6.78	1	N/A	0
3 – Malicious Code	12.27	866	8.24	280
4 – Improper Usage	13.46	232	13.29	11
5 – Scans/Probes/Attempted Access	20.23	5	N/A	0
8 – Data Loss	2.76	802	1.08	110

Source: OIG assessment of JSOC-provided Remedy tickets

We found that JSOC lacks guidance regarding the amount of time it should take to resolve a ticket. Our analysis determined that some tickets

may remain open for an extended period of time; at least one remained open for over 4 months. JSOC officials told us they may follow up with a component regarding the status of an incident or its vulnerability assessment, especially after 30 days. Although this follow up does not necessarily resolve the ticket, it provides additional oversight and a reminder to the component to resolve any lingering unresolved tickets.

JSOC officials explained that in the 3 months between our two sample periods, management continued its focus on emphasizing processes and its introduction of the "Closer" role, which designated staff as being responsible for reviewing tickets open for longer than 30 days, to decrease the time for closure.[31] JSOC officials believe this new review role has resulted in the more timely closure rate, as indicated in our analysis.

Overall, we found that the time JSOC allows an incident ticket to remain open creates the potential for unnecessary risk to the IT environment. For example, as shown in Exhibit 5, 10 percent of the tickets from the original sample and 6 percent of the tickets from the second sample were open longer than 30 days. The longer a ticket remains unresolved, the longer the vulnerability may exist and can compromise the system and its data. We recognize that JSOC has made efforts to reduce the length of time tickets remain open by adding the "Closer" role and emphasizing that components and JSOC analysts follow established processes. However, we believe JSOC should pursue additional efforts, such as conducting risk assessments to determine timeframes for opening and closing tickets, and further define and document these processes to mitigate the potential cyber security risk.

Analysis of Incident Monitoring in Remedy

We reviewed two samples of tickets to assess JSOC's incident monitoring process in Remedy. Our samples included 524 out of 1,912 resolved tickets from January 4, 2010 through June 24, 2010 and 123 out of 402 resolved tickets from September 20, 2010 through October 22, 2010. For these two samples, we reviewed documentation for resolving incidents.[32] Our analysis of both ticket samples identified

---

[31] Three JSOC technical lead staff are responsible for this role and work with both JSOC analysts and components to obtain updates and resolution.

[32] As reported earlier, we selected 2 samples of open tickets—533 out of 1,996 from January 4, 2010, through June 24, 2010, and 133 out of 512 from September 20, 2010, through October 22, 2010. However, because our analysis required resolved tickets to have documentation supporting resolution and a resolution timestamp, we reviewed 524 and 123 resolved tickets, respectively, for these time periods. The tickets not reviewed were still

weaknesses in the following areas: (1) incident follow-up; (2) category change correlation; (3) original category placement; (4) closure support; (5) reporting timeliness based on JSOC requirements; (6) reporting timeliness based on US-CERT requirements; and (7) tickets with post-resolution actions.[33] Our analysis also included a review of the level of JSOC investigative assistance provided to components when JSOC is notified of an incident. We found that JSOC provided sufficient information for components to begin their investigation, such as providing components with network information regarding their incidents.

JSOC Incident Ticket Follow-Up

JSOC does not have a policy that establishes how often it should follow up with components on open tickets. JSOC analysts are not consistent in how they follow up on incidents. The resolution process occurs on an ad-hoc basis unless an event triggers a response, such as the ticket aging 30 days, or a component initiates communication. Based on our review of the incident ticket process, we determined that follow-up should be conducted at least weekly. We selected 1 week as a baseline to verify JSOC's monitoring of open incidents and minimize risk in the IT environment. At a minimum, weekly follow-up of open tickets via e-mail or phone provides a greater assurance that both JSOC and the component are knowledgeable of an incident's status. Although the Remedy system provides each component with a "dashboard" that provides its overall ticket status, we believe that regular contact from JSOC increases the likelihood that incidents are investigated and resolved in a timely manner. Our analysis of JSOC's ticket process identified 22 percent (116 tickets out of 524 tickets) that were not followed up on at least weekly in our original sample, while we found 5 percent (6 tickets out of 123 tickets) in our second sample were not followed up on at least weekly. This indicates improvement in JSOC's processes. Exhibit 8 illustrates our review of JSOC follow-up for both samples.

---

open and unresolved at the time the sample was taken and thus we were unable to review their resolution.

[33] We use the term category change correlation to describe whether sufficient documentation existed to verify that an incident category change was warranted and supported with documented evidence for the change. Post-resolution actions include additional information added to ticket files after resolution, raising concerns over whether tickets were resolved prematurely.

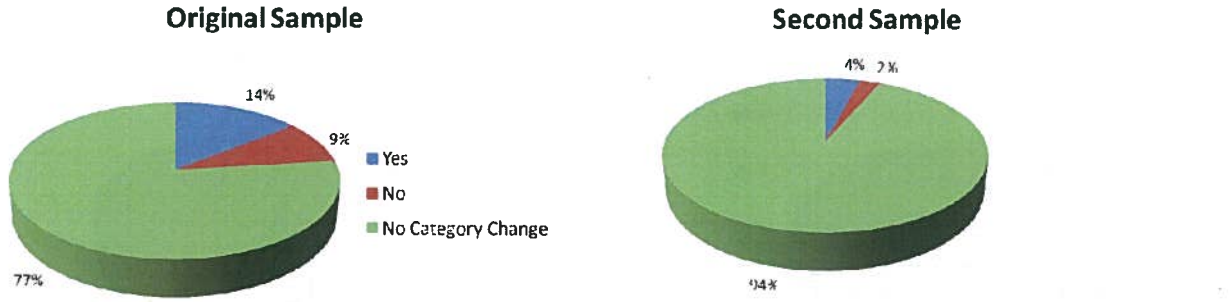
EXHIBIT 8: JSOC'S WEEKLY FOLLOW-UP OF RESOLVED INCIDENT TICKETS

Source: OIG assessment of JSOC-provided Remedy tickets

Category Change Correlation

We also analyzed incident tickets to determine whether sufficient documentation existed to verify that an incident category change was warranted and supported, meaning that the category change could be connected to a specific documented event supporting the evidence for a change. For example, we assessed whether documentation existed to reclassify a Category 6 (Investigation) incident into a reportable incident category, such as a Category 3 (Malicious Code). Category changes are used to reclassify incidents under investigation to a reportable category or to modify an existing incident ticket's reportable category based on updated information. Capturing the correlation information is necessary to determine if the JSOC analyst had sufficient reason to modify a ticket or substantiate why it may be misclassified. Misclassified tickets may increase the risk that an incident may not be reported timely and may lengthen the time the system remains vulnerable. For example, if a ticket that should be classified as Category 3 (Malicious Code, reportable in 24 hours) was reported as a Category 4 (Improper Usage, reportable in 1 week) the incident could be reported 6 days late. In order to mitigate concerns regarding ticket classification, JSOC should always document reasons for ticket category changes within Remedy. Our analysis of documentation to support a category change identified that 9 percent (46 tickets out of 524 tickets) in the original sample and 2 percent (3 tickets out of 123 tickets) in the second sample lacked appropriate documentation, such as work logs, indicating improvement in JSOC's processes. Exhibit 9 illustrates our findings.

EXHIBIT 9: DOCUMENTED INCIDENT TICKET CHANGE CORRELATION

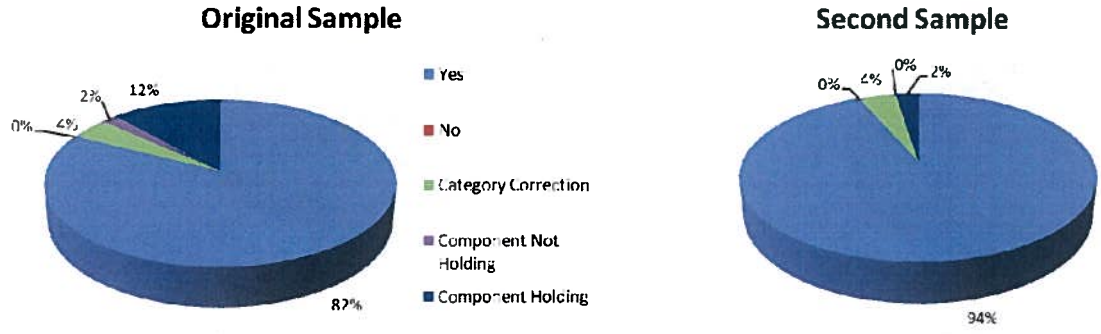


Source: OIG assessment of JSOC-provided Remedy tickets

Original Incident Classification

We determined that some incident tickets originally classified as Category 6 (Investigation) may be "held" in this category rather than investigated and classified as a categorized risk or removed as a non-event. As shown in Exhibit 10, we identified 12 percent (61 tickets out of 524 tickets) of incident tickets from the original sample and 2 percent (3 tickets out of 123 tickets) from the second sample as incidents with a potential holding status in Category 6. The exhibit category "Yes" indicates that the incident was classified correctly originally. "No" indicates that the ticket was not classified correctly. "Category Correction" indicates that the ticket's category was changed within 24 hours of opening which we consider a corrective action. "Component Holding" indicates that the ticket is missing documentation that would provide support to why the ticket remains in Category 6. "Component Not Holding" indicates that a ticket was open for longer than 7 days in Category 6 with documentation to support the need to be in the investigative category. We reviewed tickets for multiple indicators – such as a lack of communication between a component and JSOC, lack of explanation for the delay, or lack of monitoring of components needing additional time to address the incident – that contributed to a component potentially "holding" tickets in a non-reportable category. The risk with this is that cyber security vulnerabilities may remain unmitigated for an extended period of time because the clock has not started for the component to report the incident, which could lead to a lack of urgency to resolve it and prolong weaknesses throughout the network. JSOC management should provide more guidance to JSOC analysts and components regarding ticket classification and JSOC analysts should monitor tickets to prevent potential holding.

EXHIBIT 10: ORIGINAL INCIDENT CLASSIFICATION



Source: OIG assessment of JSOC-provided Remedy tickets

Closure Support

JSOC requires its analysts to document the closure of an incident. However, based on our discussion with JSOC officials, we found that no policy specifies what documentation is appropriate for closure due to the varying nature of an incident. To test the sufficiency of documentation for closure of a ticket, we reviewed incident closure documentation to determine whether it would mitigate risk and if component staff responsible for reporting the closure action were identified in the ticket. We selected documentation from JSOC's Incident Report Form for review, which includes fields for component contact information, incident details, and supporting information. We then compared this information to the NIST's *Computer Incident Handling Guide*, which provides suggested fields for closure that supported our assessment of fields we reviewed for closure.[34] Based on our analysis we determined information sufficient for closure should include, at a minimum, documentation that indicates an incident is no longer a risk and that the individual responsible for reporting a completed action is identified in the ticket. Examples of closure actions could include notification that a computer had been re-imaged, that malicious code had been removed, or that traffic being monitored was in fact from a legitimate website.[35]

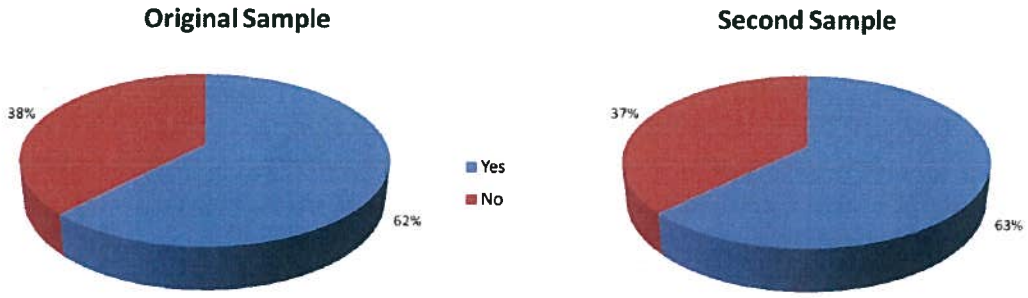
Our analysis of tickets deemed completed by JSOC found that 38 percent (199 out of 524 tickets) in the original sample and 37 percent

[34] NIST Special Publication 800-61 Rev 1, *Computer Security Incident Handling Guide*, (March 2008).

[35] Re-imaging refers to formatting the hard disk and the re-installation of the operating system and applications on a computer.

(46 out of 123 tickets) in the second sample lacked sufficient information to resolve a ticket, as shown in Exhibit 11. We also found that 5 percent (25 tickets) from the original sample and 7 percent (8 tickets) from the second sample indicated an outstanding closure action, or that an action needed to be completed before the ticket could be closed. We considered these incidents to still be at risk. An example of an incident ticket whose closure is outstanding could be a computer that has been compromised and taken off the network to be re-imaged. Although the immediate risk has been averted by removing the computer from the network, a certification from the component that the computer has been re-imaged may be pending. As a result, the computer could be mistakenly placed back on the network without re-imaging. While JSOC may be able to verify that a computer has been placed back on the network without re-imaging, it does not change the fact that an infected computer has been placed back on the network with other potentially vulnerable machines. In order to mitigate risks associated with inappropriate closure, policies should be documented to provide guidance regarding sufficient closure and to provide additional oversight on the adequacy of ticket closure documentation.

EXHIBIT 11: INCIDENT TICKET CLOSURE SUPPORT



Source: OIG assessment of JSOC-provided Remedy tickets

Timeliness in Incident Reporting

As mentioned previously, JSOC interprets US-CERT reporting guidelines for timeliness of reporting beginning when JSOC is notified of an incident by a component. JSOC provides the components the same amount of time to report incidents to JSOC as JSOC uses to comply with reporting incidents to US-CERT, as indicated by JSOC's Incident Reporting Handbook. JSOC's Incident Response Plan requires Category 6 (Investigation) incidents

to be reported periodically as information is developed.[36] For example, according to US-CERT criteria, a non-widespread Category 3 (Malicious Code) incident should be reported to US-CERT within 24 hours of detection. JSOC policy allows a component 24 hours to report the incident to JSOC, although informally, JSOC requests components to immediately report incidents to JSOC. Further, although JSOC requests its analysts to report the incident to US-CERT immediately, once JSOC receives an incident ticket from a component, it also allows itself 24 hours to report the incident to US-CERT. Thus, JSOC allows DOJ a total of 48 hours from first detection to report a non-widespread Category 3 (Malicious Code) to US-CERT, whereas a strict interpretation of US-CERT guidance would require this incident to be reported within 24 hours of detection.

We analyzed incident tickets based on both an assessment of US-CERT's reporting guidance and JSOC's reporting practices. Exhibit 12 illustrates ticket timeliness based on the date a reportable category was identified, including when a Category 6 (Investigation) incident transferred into a reportable category, and who is responsible for the delay based on JSOC's reporting process. Our review of JSOC's timeliness in reporting incidents to US-CERT from the time JSOC receives an incident report found that 14 percent (76 out of 524 tickets) in the original sample and 4 percent (4 out of 123 tickets) in the second sample were not reported to US-CERT in accordance with JSOC requirements.[37]

We furthered reviewed JSOC's requirements for component to JSOC reporting and found that a majority of these tickets—66 percent (347 out of 524 tickets) in the original sample and 86 percent (106 out of 123 tickets) in the second sample—were not timely because components did not report the incident to JSOC in accordance with JSOC's requirements.[38]

Within the overall reporting process, including incident notification from components to JSOC and JSOC reporting to US-CERT, we found that

---

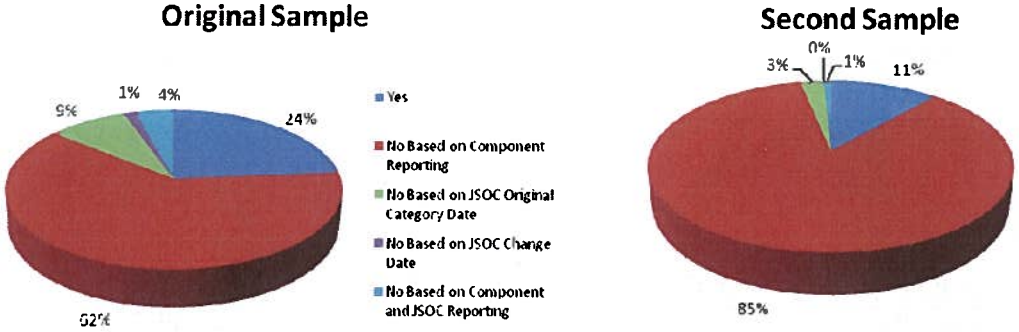
[36] We determined that Category 6 (Investigation) incidents should be assessed to confirm whether an incident was reported within 24 hours, due to the potential risk of unconfirmed incidents and based on the vague guidance from JSOC regarding periodic reporting. Based on our assessment, we identified 14 Category 6 incidents to be in non-compliance with the reporting timeframe.

[37] The number of tickets and percentage is the sum of all "No-JSOC Original, No-JSOC Change, and No-Comp and JSOC" categories.

[38] The number of tickets and percentage is the sum of all "No-Comp and No-Comp and JSOC" categories.

76 percent (396 out of 524 tickets) in the original sample and 89 percent (110 out of 123 tickets) in the second sample were not reported to US-CERT in accordance with JSOC's requirements.[39] Our analysis illustrates that despite improvements in JSOC's reporting to US-CERT, weaknesses in JSOC's process for reporting to US-CERT remain since delays in reporting tickets still occur from both components to JSOC and JSOC to US-CERT. JSOC follows DOJ's Computer System Incident Response Plan, which identifies timeframes for reporting incident tickets.[40] The timeframes established in this plan are the same as in the guidance issued by US-CERT, shown in Exhibit 1. Additional oversight and written requirements should be addressed to both JSOC analysts and components by JSOC management to ensure both are reporting based on requirements.

EXHIBIT 12: OVERALL TIMELINESS FOR REPORTING INCIDENTS USING JSOC CRITERIA



Source: OIG assessment of JSOC-provided Remedy tickets

As shown in Exhibit 13, our analysis of the timeliness of incidents reported based on a strict interpretation of US-CERT guidelines found that 78 percent (408 out of 524 tickets) in the original sample and 93 percent (114 out of 133 tickets) in the second sample were not reported timely. As mentioned previously, US-CERT has been unable to provide specific guidance regarding the definition of detection date for reporting incidents to US-CERT. Rather, US-CERT indicated that DOJ should perform a risk assessment to determine its interpretation of US-CERT guidance. Based on a lack of a documented risk assessment at JSOC for using its receipt of a reportable

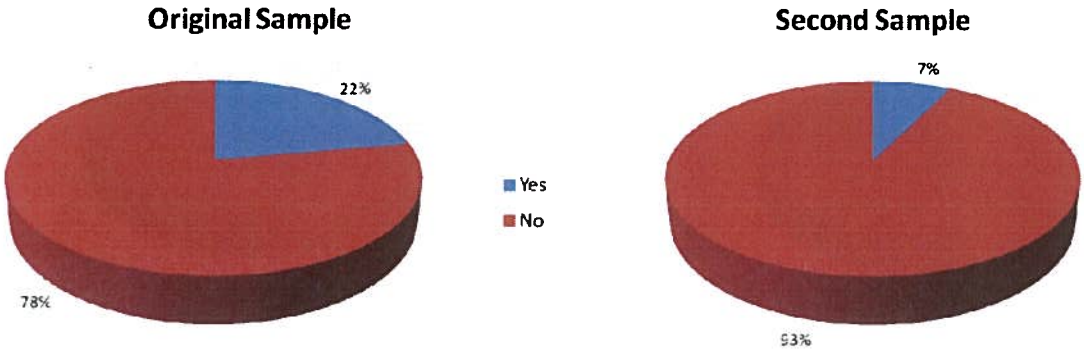
[39] The number of tickets and percentage is the sum of all "No-Comp, No-JSOC Original, No-JSOC Change, and No-Comp and JSOC" categories.

[40] The Incident Reporting Handbook also notes that components are expected to report events that occur after hours within the established timeframe.

category incident as the starting point for reporting to US-CERT, rather than the component's detection date, a strict interpretation of US-CERT's timeframe was used for this analysis.

We considered a strict interpretation of US-CERT guidelines to be the total time, beginning with the detection date of an incident in a reportable category at the component or JSOC, and the date JSOC subsequently reported the incident to US-CERT. As a result, more incident tickets are not reported timely using a strict interpretation of US-CERT guidance than using JSOC's current process.[41] Therefore, it appears that a risk assessment should be performed to account for the additional time, as incidents potentially exist without being reported and monitored by JSOC for longer than necessary.

EXHIBIT 13: OVERALL TIMELINESS FOR REPORTING INCIDENTS USING STRICT INTERPRETATION OF US-CERT GUIDANCE



Source: OIG assessment of JSOC-provided Remedy tickets

Post-Resolution Ticket Activity

We observed occasions where additional information was added to ticket files after resolution, raising concerns over whether tickets were resolved prematurely. We identified notations in the ticket files indicating that information such as e-mail correspondence or analysts' notes added post resolution would contain evidence required for sufficient closure. JSOC officials told us some circumstances may warrant additional information after resolution. These can include further actions taken by components or additional information obtained, such as recovery efforts or analysis of data loss, beyond a ticket's original closure date. In general this information is

[41] We were unable to fully determine the effect of using JSOC's process and US-CERT's timeframe guidelines since incidents that exceeded the reporting timeframe based on JSOC"s process would also fail US-CERT's reporting timeframe.

self-reported to JSOC by the component, although there are instances in which JSOC may ask the component to provide more information. In addition, automated system entries due to search queries may be automatically placed in a ticket file's work log, updating the last ticket modification date. While we did not perform a comprehensive review of the two samples for post-resolution activity, in our testing we found that for a few incidents, evidence documenting resolution was not added until after the ticket had been classified as resolved. We believe such instances demonstrate a risk that JSOC may be prematurely closing an incident prior to sufficient documentation, whether intentionally or in error.

We found that of the entry fields in Remedy, the note field – which includes narrative information – does not include an auditable entry.[42] We could not determine if information added to the note field in support of ticket resolution was added prior to or after the resolution of a ticket. As stated previously, we also identified tickets that were closed but required future action, such as the re-imaging of a computer that had yet to occur. Therefore, we believe that an incident ticket should not be considered closed or resolved until sufficient closure information is received from the component, such as confirming that re-imaging has occurred, rather than indicated as closed but pending future action. Policies and procedures should be developed by JSOC regarding post-resolution modifications to ensure modifications that occur are identifiable and auditable and that sufficient information for closure is provided prior to post-resolution modification.

We identified insufficient guidance in JSOC's incident monitoring processes. Based on our analysis of both samples, we determined that incidents reported in Remedy lacked sufficient information to ensure appropriate monitoring and resolution in the areas of evidence, category change correlation, original category classification, closure information, and post-resolution modification. We identified concerns with timely incident reporting both from the component to JSOC and JSOC to US-CERT. Without policy guidance, sufficient supporting documentation, and adherence to policies, we are unable to assess whether all incident tickets have been adequately tracked and if security conditions have been properly mitigated and addressed.

---

[42] The note field in Remedy allows analysts to input information regarding an incident, including information regarding resolution. It is one of several fields, along with the status and uploaded documentation fields, used to provide pertinent investigation information. The note field entry allows unlimited characters and JSOC does not currently enable this field to be auditable due to its concerns regarding this feature.

Tracking Widespread Incidents

US-CERT officials informed us that the definition of a widespread incident should be decided by DOJ based on its determinations of risk thresholds and other factors associated with this category of outbreak. JSOC officials informed us that JSOC's Worm Outbreak Incident Response Playbook gives guidance on the definition and treatment of widespread incidents in DOJ. However, our review of the Worm Outbreak Incident Response Playbook found that it does not explicitly define widespread incidents. Rather, it provides general guidance on how to analyze and respond to a large scale outbreak of a worm.[43] We believe JSOC should develop specific guidance that defines widespread incidents for all malicious incidents at DOJ.

US-CERT guidelines require that widespread malicious code be reported within 1 hour of detection or discovery across the agency. JSOC's Remedy system includes a reportable field for widespread incidents. However, JSOC officials told us that its analysts do not use this field in Remedy. Instead, JSOC officials informed us that JSOC prefers to notify US-CERT officials by e-mail or phone rather than track the widespread incidents within Remedy. JSOC officials were unable to provide us with a policy documenting their process for tracking and reporting widespread incidents.[44]

Because JSOC does not document widespread incidents in Remedy, we are unable to determine whether these incidents are reported on time, monitored effectively or how many have been identified. As a result, JSOC may not be meeting US-CERT guidance for widespread incident reporting and may not have an accurate count of infected machines, which may result in delays in mitigating risk. JSOC should develop a methodology that specifically documents and tracks widespread incidents.

Assessment of JSOC Policies

We reviewed JSOC's incident response and coordination policies to understand how JSOC manages incidents and monitors networks. Multiple policies exist to explain the different elements of incident handling at JSOC,

---

[43] NIST SP 800-61 rev 1 *Computer Security Incident Handling Guide* defines "worms" as self replicating programs that are completely self-contained and also self-propagating. Worms take advantage of vulnerabilities and weaknesses in the system to waste network resources and perform other malicious acts to compromise the network.

[44] In our discussions with JSOC, we were informed that the DOJ has been the subject of widespread malicious code attacks such as the publicly reported 2009 virus that struck the FBI and USMS.

including the Incident Reporting Handbook and standard operating procedures. Appendix III lists 22 JSOC policies, plans, and procedures we reviewed. These policies cover a wide range of network security monitoring initiatives including network forensics, incident communications, cyber threat analysis, and incident management tools.

We found that four of JSOC's policies were not finalized and that some of these may not include information that reflects current operations. Specifically, we found that the SCIF Secret Monitoring SOP, SCIF Top Secret Monitoring, DoS [Denial of Service] Cyber Threat Handbook, and the Incident Reporting Handbook were not finalized.[45] We requested updates for these documents and were told that policies were currently being reviewed by JSOC officials and that they would provide us with updates. As of May 2011, we have received updates to the DoS Cyber Threat Handbook and the Incident Reporting Handbook, however, we found that these were not signed and both SCIF policies have not been finalized.

In our review of JSOC's Incident Reporting Handbook, we found that Category 8 (Data Loss) tickets were not identified as reportable. JSOC officials told us that it prefers to use Category 8 to internally track tickets that are actually Category 1 (Unauthorized Access) tickets in terms of US-CERT reporting requirements. The Incident Reporting Handbook does not explain that Category 8 tickets should be included in Category 1 and are reportable to US-CERT.

Another undocumented incident activity is JSOC's "Closer" role, or staff responsible for reviewing tickets more than 30 days old in Remedy. As explained above, beginning in June 2010, three JSOC staff act as "Closers" who review ticket queries that identify open and aged incidents and work with the component to close the tickets. As of May 2011, JSOC had not documented the "Closer" role as part of its Quality Assurance Program.

We believe these examples of policies that potentially include conflicting or lack of current information regarding incident response activity present risk to DOJ's environment. They may result in actions performed not in accordance with current policies or guidance, which we believe increases the risk to DOJ's incident management process due to inaccurate or inconsistent performance of these procedures. We believe policies should be updated and finalized to reflect current operations and components and JSOC analysts should be aware of any updates.

---

[45] As mentioned previously, although JSOC relies on components to maintain their classified systems, JSOC performs some classified system work for JMD. As a result, the policies we reviewed included those pertaining to classified systems.

JSOC Adherence to US-CERT Guidance

We met with US-CERT officials to gain their perspectives on JSOC's ability to report incidents according to US-CERT's guidance. These officials told us they are not aware of any issues regarding the timeliness or comprehensiveness of JSOC's reporting to US-CERT. However, these officials informed us that US-CERT currently lacks authority to formally issue requirements or monitor compliance. Instead, US-CERT provides information sharing and collaboration regarding cyber security. Subsequently, US-CERT can only provide recommendations for addressing policy, such as performing risk assessments of certain processes. US-CERT officials stated that their guidance to JSOC and other agencies regarding incident reporting is to perform a risk assessment to determine how quickly to report various types of incidents to US-CERT, including widespread incidents. As previously discussed, JSOC does not strictly interpret US-CERT's reporting guidance.

II. JSOC Efforts to Support and Coordinate with Components

We reviewed the effectiveness of JSOC's coordination with components and JSOC's efforts to support the components. We also analyzed the status of information feeds from the components to JSOC, services provided by JSOC to the components, and reporting information between JSOC and the components, as well as spoke with officials from 13 DOJ components regarding their coordination with JSOC. Many components and offices have noticed an improvement in communication and coordination with JSOC. However, our audit raises concerns about how well JSOC receives necessary incident information from components, components' awareness of JSOC services, and components' commitment to following DOJ's Computer System Incident Response Plan.

We found that: (1) 6 out of 32 components or offices have not fully provided information feeds to JSOC, resulting in JSOC not having a comprehensive view of the network; (2) at least 2 components were not aware of the assistance JSOC offers and therefore did not take advantage of JSOC's services; and (3) the FBI's process of not reporting to JSOC incidents that it categorizes as under investigation disregards policy requirements provided by OCIO and potentially allows vulnerabilities—or susceptibility of DOJ's computer systems to intrusion or attack—to remain at risk longer than necessary.

Component Information Feeds and External Connections

As previously discussed, one of JSOC's primary roles is to monitor cyber activity within DOJ. Thus JSOC relies on information provided regularly from components and offices. This information is submitted through four separate information feeds. An information feed is a direct, real-time or near real-time electronic data input of relevant security monitoring and auditing data, such as firewall event logs, intrusion detection or prevention system alerts and logs, network and desktop antivirus event logs, and content scanning and filtering system logs. These information feeds are the: Intrusion Detection System (IDS), Antivirus (AV), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS).

- IDS—provides information captured by the components' intrusion detection system, which logs malicious activity or policy violations.

- AV—used to detect and remove malware, which may include computer viruses, spyware, and adware.

- DCHP—acts a central database in tracking which computers are connected to the DOJ network and automatically assigns Internet protocol (IP) addresses, which helps identify individual computers or other network devices such as printers.

- DNS—maps a website domain name into a numeric IP address.

These feeds contain aggregated activity data that allow JSOC to conduct an effective and efficient level of monitoring.

We reviewed components' status with providing these feeds to JSOC, which included components' compliance with integrating any external Internet connections into the Trusted Internet Connection (TIC). As discussed earlier in this report, the TIC allows for a centralized gateway for JSOC to more easily monitor and identify malicious traffic and strengthen its incident response capabilities.

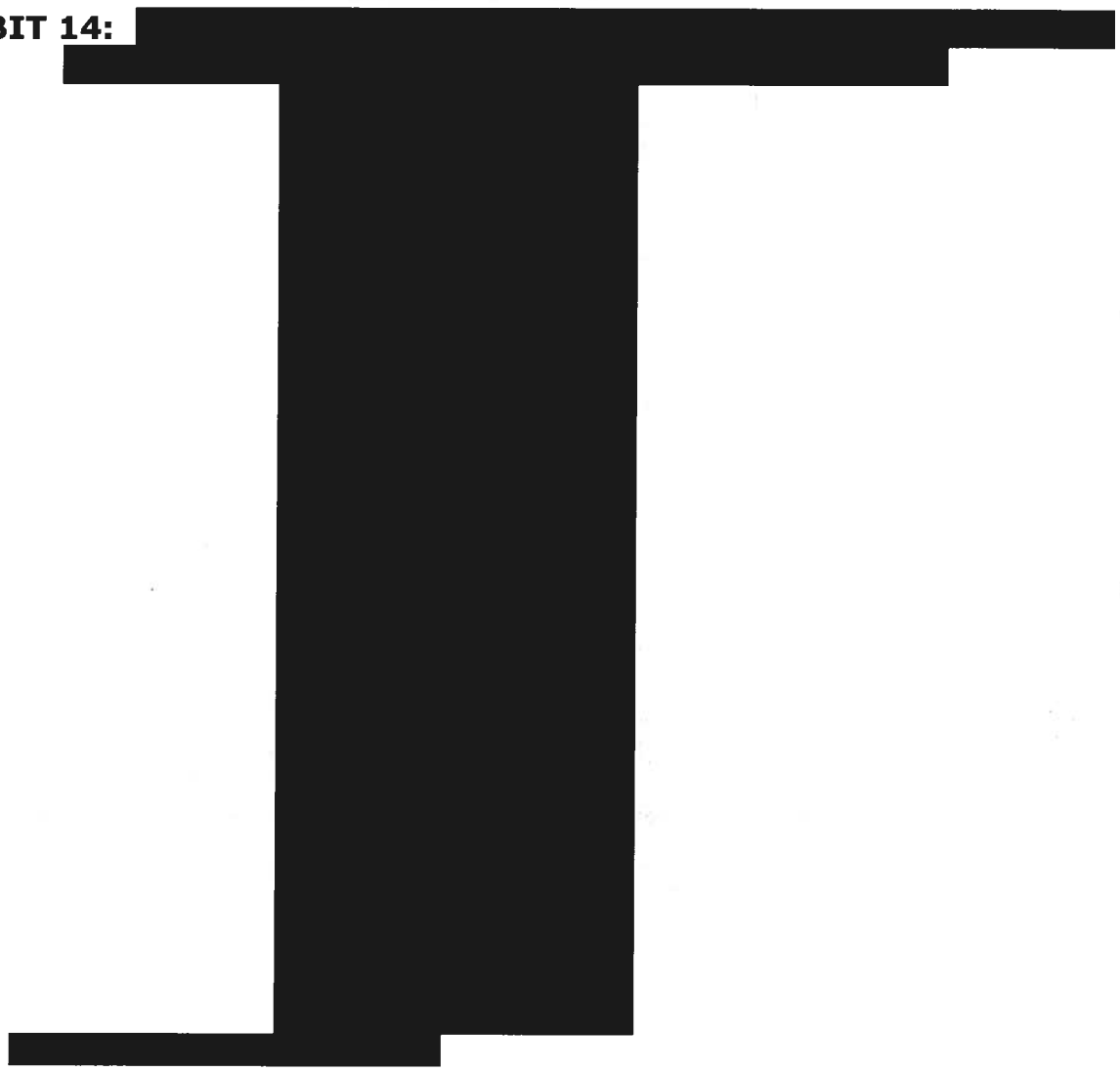
Component Information Feeds

From components' information feeds, JSOC becomes aware of and is able to correlate common network activities to gain a better understanding of what is occurring on the network for more effective monitoring. As previously mentioned, JSOC uses [redacted], a Security Information Management tool, to compile and correlate network activities from the various internal information data feeds. During our audit, JSOC requested DOJ components to provide certain information feeds to enhance JSOC's situational awareness and effectively detect activity. JSOC requested components to provide Intrusion Detection System, Antivirus, Dynamic Host Protocol and Domain Name System feeds by March 2010. Yet, as of May 2011, six components were still working to provide JSOC with all requested information feeds. Some components have run into problems with IDS, AV, and DHCP feeds and have experienced functional and operational issues involving coordination with multiple entities and difficulties in sending information.

Exhibit 14 illustrates the status of the various information feeds provided by components to JSOC as of May 3, 2011. Information feed activity is assessed according to six classification categories. "Reporting" (green) designates that information is being or has been reported. "In

progress" (yellow) denotes that the component is currently working but has not yet transmitted the information to JSOC. "No Connector" (orange) means no available connector exists to provide the information to JSOC. Components without connectors are identified as complete as no further work can be done on it. "No Progress" (red) indicates that no steps have been taken towards providing the requested information. "Survey: no product" (black) designates that the component is not capturing the information requested through its own monitoring, and therefore cannot provide the data to JSOC. "Feeds Incomplete" (white) denotes that the component has not provided all available feeds to JSOC.

EXHIBIT 14: [redacted]



Source: [redacted]

As shown in Exhibit 14, the six components or offices identified as working to provide requested feeds (except for Domain Name Systems (DNS)) are the Civil Division (CIV), Executive Office for United States Attorneys (EOUSA), FBI, OIG, USMS and United State Parole Commission

(USPC). In addition, 18 components or systems have yet to provide JSOC with requested DNS feeds. According to JSOC officials, this is in part due to JSOC's inability to review and correlate the volume of DNS logs until its upgrade of [redacted], which is not anticipated until August 2011, is complete.[46] Until then, DNS feed status does not affect a component's status on compliance.

Based on our review of these information feeds, we found that the FBI is the only component that had not provided any information feeds to JSOC during our audit timeframe. Based on emails exchanged between JSOC and the FBI, difficulties for integration are due to the challenges the FBI and JSOC faced connecting the FBI's separately managed network to DOJ's primary network. According to JSOC officials, JSOC has been attempting to obtain feeds from the FBI since July 2010. It appears that JSOC and the Justice Data Center in [redacted], which maintains DOJ's networks, have provided the FBI with a circuit path for the FBI's Enterprise Security Operations Center's (ESOC) connectivity. However, technical issues at both the Justice Management Division (JMD) and the FBI caused the delay in providing feeds from ESOC to JSOC. The FBI submitted a change request in June 2010, which was approved in October 2010, to allow feeds for JSOC's security monitoring and continuing efforts in this endeavor. As of May 23, 2011, the FBI's IDS feed was being received by JSOC.

External Connections

As of March 2011, four components (ATF, BOP, FBI, and FPI) maintained a total of 13 external connections.[47] An update from JMD in May 2011 stated that only three components (ATF, BOP, and FBI) continued to have [redacted][48]. JSOC's

[46] JSOC is not expected to acquire 100 percent of component DNS feeds before the second quarter of fiscal year 2012.

[47] These external connections link communications between DOJ components and their non-DOJ partners, which include both law enforcement and businesses.

[48] [redacted]

monitoring of this traffic is dependent upon a component's information feeds and whether the traffic is forwarded through to other components within the network.

JSOC's lack of access to information from component network activity reduces its ability to monitor the overall security posture of DOJ's networks effectively and efficiently. Similarly, the existence of 10 network connections outside the TIC limits JSOC's ability to monitor this activity itself, instead having to depend on the component to do so. We believe this potentially increases vulnerability in DOJ's information security environment because it provides access points for malicious attacks that may not be effectively monitored and limits JSOC's awareness of the environment.

Component Awareness of JSOC Capabilities

We interviewed 13 DOJ components and offices regarding their interaction with and understanding of JSOC and its capabilities.[49] Each of these components indicated an improvement in incident response operations under the current JSOC leadership related to processes and communications. Officials from these components and offices told us that JSOC is generally receptive to discussions with them.

However, we found that not all components had an equal understanding of JSOC's services. At least two components were unaware of specific IT forensic analysis services offered by JSOC. JSOC officials informed us they use various ways to communicate JSOC's services to components, from handouts to monthly meetings. We found that while JSOC's handouts included forensic analysis as one of its services, these materials did not explain how a component could request the service. As a result, some components understood that the forensic services advertised were JSOC-initiated requests for investigation of hard drives rather than for components to request forensic services from JSOC. Components that wished to take advantage of forensic service would either have to find another provider, develop in-house capabilities or not complete forensic analysis.

Officials from one component informed us that they have not seen any directive explaining JSOC's full authority and capability, and that this presents a challenge when JSOC requests new processes of the component.

---

[49] These components and offices are: the FBI; EOUSA; DEA; OJP; ATF; BOP; COPS; Environment and Natural Resources Division; Executive Office for Immigration Review; Federal Prison Industries, Inc.; National Drug Intelligence Center; USMS; and Wireless Management Office.

We also could not locate a policy or memorandum that addresses JSOC's official creation and its authority. JSOC officials told us that its responsibilities for IT security are outlined in IT Security Order DOJ 2640.2F, which provides overall guidance for DOJ's IT policy, responsibility, and authority. Although the Security Order does not specifically identify JSOC, it provides a preliminary basis for DOJ IT security requirements as a whole and the rationale for JSOC's establishment.

The components we met with had generally positive feedback regarding JSOC's services. However, officials cited specific areas where they could benefit from increases in JSOC services. Several components would like JSOC to provide them with additional information regarding current malware trends. Other improvements components mentioned included increasing the blocks of certain Internet sites, the availability of TIC log information, and additional post-forensic analysis on incidents. Components also mentioned the desire for increased training, specifically more simulations and the availability of web-based training. In addition, components cited the need for web-based meeting websites and additional [redacted] capabilities, such as console viewing.

JSOC should evaluate and address component concerns regarding additional services and lack of full awareness of current services. This increase in component understanding may assist JSOC's efforts in securing DOJ's network and improving interaction with components.

The FBI's Reporting to JSOC

We interviewed FBI officials regarding their coordination with JSOC for incident reporting purposes. As previously mentioned, [redacted] and a separate Enterprise Security Operations Center (ESOC). However, the FBI is still required to report incidents to JSOC because JSOC is responsible for reporting all DOJ incidents to US-CERT. ESOC officials informed us that they use several internal ticketing systems to track incidents under investigation, and that only upon classifying an incident into a reportable category does ESOC report the incident to JSOC.[50] When we asked JSOC officials whether ESOC reports any Category 6 (Investigation) incidents to JSOC, we were told they did not believe any had been reported

[50] During our review, we identified one incident in our sample dealing with data loss (a letter containing PII) that was reported as a Category 6 FBI incident. However, that incident was not reported by ESOC. Instead, it was reported to JSOC by the FBI's Criminal Justice Information Services. This was the only incident in our sample reported as a Category 6 FBI incident.

by ESOC. According to DOJ's Computer System Incident Response Plan, a potential incident under investigation should be reported periodically to JSOC as information is developed and as soon as detected if the incident includes data loss.[51] JSOC officials informed us that there is no formal agreement between it and the FBI to not report incidents under investigation.

In a follow-up meeting with ESOC, ESOC informed us that it submitted 16 Category 6 incidents, out of 646 incidents, to JSOC during our sample time period. While ESOC indicated it has reported a limited number of Category 6 incidents, ESOC officials informed us that there is no requirement to report Category 6 incidents based on what JSOC has provided them, and they were not inclined to do so due to the voluminous use of Category 6 to triage unconfirmed incidents that they believe are not relevant to JSOC's purposes. When we informed ESOC that JSOC had provided us with the OCIO- distributed DOJ-wide DOJ Computer System Incident Reporting Plan that indicated that periodic reporting was required, ESOC notified us that it has not received this plan and that the plan contradicts information provided by JSOC in its incident categories chart.

The FBI provided a chart detailing JSOC reportable categories, which is available on JSOC's website. This chart, labeled JSOC Incident Categories, defines the reporting timeframe for Category 6 incidents as "Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated." These guidelines are similar to the US-CERT chart containing incident reporting guidelines, with the addition of Category 8, and provide the same reporting timeframes as US-CERT (see Exhibit 1 for US-CERT chart). JSOC's website provides no context for the categories to determine if the chart is applicable to components or for JSOC's use.

The DOJ Computer System Incident Response Plan that was provided to us by JSOC is also available on JSOC's website. This plan indicates that it should serve as the foundation for each component's computer security incident response process. The plan determines the reporting timeframe for Category 6 incidents to be "Periodically as information is developed. This category is for each Component's use in categorizing a potential incident that is currently being investigated." The plan clearly delineates that the reporting requirements in this chart are for components to JSOC.

---

[51] JSOC provides policy and guidance to components regarding their reporting requirements. The DOJ Incident Response Plan provides information to both the components and JSOC regarding required actions and responsibilities. This document is available on the DOJ Intranet for review and as a basis for component incident response plans.

We also found that upon a closer review of the JSOC Incident Categories chart provided by the FBI, the chart indicated that the reporting timeframes were at Agency level. This differs from the chart in the DOJ Computer System Incident Response Plan that indicates the timeframes are at the Component level. Based on this review, it is our judgment that the FBI-provided plan is at the Agency, or JSOC level, for DOJ reporting as an Agency rather than at the FBI reporting to JSOC level. However, at a high level review this may be unclear to the reader. We believe that the discrepancy between the two plans may lead to a problem in discerning the correct reporting requirements and should subsequently be clarified.

We have several concerns with the FBI's process of not reporting Category 6 incidents due to the potential lack of efficiency from a failure to share information between ESOC and JSOC. Because ESOC's process does not provide JSOC with information on incident tickets ESOC categorizes as under investigation, JSOC may not have an understanding of the full scope of potential security risks within DOJ, nor can JSOC monitor and help resolve these incidents, or relate them to any similar incidents under investigation in other components. While the FBI informed us it has reported a small number of Category 6 incidents, the process to not report them is inconsistent with this action and brings into question whether the FBI is providing sufficient information to JSOC regarding Category 6 incidents. Lacking more coordination between JSOC and ESOC, the timely identification and resolution of an incident and mitigation of risk may be hampered, thus increasing the threat to the network. Also, FBI incident tickets reported to JSOC after classification prevent JSOC from conducting oversight of the overall aging of a ticket. Given ESOC's use of multiple reporting systems, the lack of reporting of Category 6 incidents to JSOC, and JSOC's limited view of FBI information feeds, we question whether ESOC is reporting all incidents to JSOC. This may prevent JSOC from having a full understanding of all potential incidents within DOJ, which may delay resolution of DOJ-wide issues. Conversely, without coordination with JSOC, the FBI may delay resolution of its incidents because it does not have the benefit of JSOC's knowledge gained from its oversight of DOJ computer networks. This risk may be lessened, however, if the FBI reports incidents under investigation and provides all feeds to JSOC. JSOC should continue efforts to ensure that the FBI's ESOC provide it with Category 6 incidents based on agreed upon requirements for Category 6 incidents that would be relevant to JSOC's monitoring and in what periodic timeframe.

Conclusion

Overall, JSOC has processes and procedures that appear to provide effective network monitoring on network traffic and information feeds received. JSOC also provides incident response coordination with DOJ components and reports to US-CERT. However, based on our analysis, there are several improvements that can be made to provide an additional level of incident monitoring capabilities and component cooperation, such as improved incident ticket processes, detailed policy updates, and additional support for integration of component processes with JSOC.

Our review of JSOC's capabilities and operations identified programmatic concerns regarding timeliness. Specifically, we believe the timeframes for opening and resolving tickets need to be improved to mitigate potential risks of vulnerabilities remaining within the network for extended periods of times, and to report to US-CERT within a timely manner. We also identified weaknesses in the following incident ticket areas: (1) incident follow-up; (2) category change correlation; (3) original category placement; (4) closure support; (5) reporting timeliness based on JSOC requirements; (6) reporting timeliness based on US-CERT Requirements; and (7) tickets with actions post-resolution. These weaknesses provide a lack of assurance that incidents are being appropriately monitored and documented to mitigate security risks. During our analysis of Remedy tickets, we also found that JSOC did not explicitly define a widespread incident or the processes to track a widespread incident. This may result in JSOC not meeting US-CERT's guidance for widespread incidents. Further, our analysis identified JSOC policies that need to be updated so as to prevent inconsistent processes and practices that may also result in an increased risk to DOJ's incident management process.

During our review of JSOC's coordination with components, we found that six components have yet to provide JSOC with all available feeds to enable effective and efficient network monitoring and event correlation. We also identified that at least 2 out of 13 components were not fully aware of all of JSOC's services, limiting their ability to take advantage of all that JSOC offers. Our review also found that the FBI's process to not report Category 6 incidents to JSOC due to unclear guidance t may prevent JSOC from having a comprehensive view of the network and potentially allowing incidents to remain uncategorized and allow the IT environment to remain vulnerable for an extended period of time.

Recommendations

We recommend that JMD ensure JSOC:

1. Establish and document guidelines regarding the timeframe of incident reporting based on the risk assessment of US-CERT reporting requirements regarding incident detection for both component to JSOC and JSOC to US-CERT reporting.

2. Perform and document a risk assessment on each category risk to determine acceptable timeframe for closure of an incident.

3. Document oversight and follow-up of open incident tickets at least weekly for all US-CERT-reportable incidents and for incidents under investigation.

4. Document reasons for ticket category changes within Remedy.

5. Provide additional guidance regarding Remedy ticket classification to JSOC analysts and components to ensure awareness of appropriate category placement.

6. Document policies regarding required information for closure.

7. Ensure Remedy tickets include sufficient documentation for closure.

8. Provide additional written requirements to both JSOC analysts and components regarding reporting timeframes and ensure reporting is based on requirements established.

9. Improve monitoring through JSOC's Quality Assurance Program and documentation that supports oversight of the Remedy Ticket lifecycle; including categorization, follow up and resolution.

10. Document policies and procedures for post-resolution modifications.

11. Ensure that any modifications that occur post-resolution are easily identifiable and that non auditable modifications are restricted from being modified post-resolution.

12. Define, in detail, "widespread" incidents for all malicious incidents at DOJ.

13. Document detailed methodology of tracking "widespread" incidents in Remedy and track these incidents in Remedy to report to US-CERT.

14. Finalize all policies and update policies to reflect current operations including defining JSOC reportable sub-categories on all applicable documents and the inclusion of the "Closer" role.

15. Ensure JSOC analysts and components are aware of updates to policies.

16. Obtain system feeds from all DOJ components to JSOC for review and trending purposes.

17. Determine and evaluate component needs and areas for improved JSOC support services.

18. Continue and improve providing information to components regarding all JSOC services and responsibilities.

19. Review and update JSOC policies to clarify potentially conflicting information regarding reporting of Category 6 incidents.

20. Determine a policy regarding appropriate periodic reporting for Category 6 incidents received from components.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards,* we tested as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of JSOC's internal controls was *not* made for the purpose of providing assurance on its internal control structure as a whole. JSOC's management is responsible for the establishment and maintenance of internal controls.

As discussed in the Findings and Recommendations section of this report, we identified deficiencies in JSOC's internal controls that are significant within the context of the audit objectives and based upon the audit work performed that we believe could affect JSOC's ability to monitor the Department of Justice's network.

Because we are not expressing an opinion on JSOC's internal control structure as a whole, this statement is intended solely for the information and use of the JSOC and the Department of Justice. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, selected transactions, records, procedures, and practices, to obtain reasonable assurance that JSOC's management complied with federal laws and regulations, for which non-compliance, in our judgment, could have a material effect on the results of our audit. JSOC's management is responsible for ensuring compliance with federal laws and regulations applicable to the information security controls. In planning our audit, we identified the following laws and regulations that concerned the operations of the JSOC and that were significant within the context of the audit objectives:

- NIST SP 800-53 rev 2;
- NIST SP 800-61 rev 1;
- NIST SP 800-83;
- NIST SP 800-86;
- NIST SP 800-94;
- Information Technology Security (DOJ Order 2640.2F);
- DOJ IT Security Standards; and
- US-CERT Federal Reporting Guidelines

Our audit included examining, on a test basis, JSOC's compliance with the aforementioned laws and regulations that could have a material effect on JSOC's operations. We interviewed key personnel within the JSOC and a sample of components, as well as performed a physical review on selected JSOC Incident Response Tickets. We contacted a sample of federal agencies to discuss their Security Operations Centers. We also visited US-CERT to discuss their operations and DOJ compliance.

As discussed in the Findings and Recommendations section of this report, we found excessive timeframes for opening and closing Remedy tickets; multiple Remedy tickets used to track incidents did not include complete and accurate information, nor were they monitored or closed in a timely manner; widespread tickets are not sufficiently defined; and policies do not reflect operations. Additionally, improvements need to be made regarding the provision of network feeds from components to JSOC and inclusion of external Internet connections to the TIC; the communication of JSOC's services to components; and the FBI's reporting of incidents.

OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit objectives were to determine: (1) JSOC's capabilities to prevent, identify, monitor, and respond to intrusion incidents; and (2) the effectiveness of the exchange of incident information and cooperation between JSOC and DOJ components.

The audit covered a 10-month period from June 2010 through March 2011. We performed our fieldwork on-site at JSOC's facility in Washington, D.C., and conducted site visits to components in the Washington, D.C., Metropolitan Area; Johnstown, Pennsylvania; and Columbia, South Carolina. During the audit period, we interviewed JSOC personnel and component SOCs and IR Teams with responsibilities related to incident response, vulnerability management, TIC integration, and general SOC operations. Within DOJ we interviewed the following components and offices: the Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Bureau of Prisons; Office of Community Oriented Policing Services; Drug Enforcement Administration; Environmental and Natural Resources Division; Executive Office for Immigration Review; Executive Office for United States Attorneys; Federal Bureau of Investigation; Federal Prison Industries Inc.; National Drug Intelligence Center; Office of Justice Programs; and Wireless Management Office. We reviewed all SOCs as identified by JSOC and selected a sample of IR teams from components and offices of various sizes.

We met with officials from the Department of Agriculture, Department of Energy, and Department of State to discuss SOC implementation efforts. We also met with officials from US-CERT to discuss its operations and DOJ's compliance with US-CERT's guidance.

During the course of the audit, we selected two samples of Remedy tickets based on indicators of delayed reporting. We initially sampled 533 out of 1,996 incident tickets that were open between January 4 and June 24, 2010. Based on review of this sample and discussions with JSOC management regarding improvements to their processes, we selected a second sample of 133 out of 512 incident tickets open between September

20 and October 22, 2010 to determine improvement of its processes. In both samples, our review included verifying timeliness of reporting, appropriate investigation, and monitoring of open tickets. Ticket samples were based on the length of time between detection date and report date to US-CERT. Tickets that exceeded timeframes specified by US-CERT based on those dates were deemed potentially indicative of JSOC monitoring and reporting issues. A subsection of tickets reviewed were assessed to have been in investigative status for a period of time, which increased the timeframe the ticket was open before reporting to US-CERT. Subsequently, not all tickets selected had delayed reporting timeframes. As we did not use a statistical sample, these results cannot be used to project to an entire population.

ACRONYMS

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BOP	Federal Bureau of Prisons
COPS	Office of Community Oriented Policing Services
DEA	Drug Enforcement Administration
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DNS	Domain Name System
DOJ	Department of Justice
DOJCERT	Department of Justice Computer Emergency Readiness Team
ENRD	Environment and Natural Resources Division
EOIR	Executive Office for Immigration Review
EOUSA	Executive Office for United States Attorneys
ESOC	Enterprise Security Operations Center (FBI)
FBI	Federal Bureau of Investigation
FPI	Federal Prison Industries, Inc.
ITSS	Information Technology Support Services
JMD	Justice Management Division
JSOC	Justice Security Operations Center
NDIC	National Drug Intelligence Center
OIG	Office of the Inspector General
OJP	Office of Justice Programs
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SOP	Standard Operating Procedures
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team
WMO	Wireless Management Office

JSOC-PROVIDED POLICIES, PLANS, AND PROCEDURES REVIEWED

01-Communication Standard Operating Procedure (SOP)
02-Compromise Alert Notification SOP
03-Remedy SOP
04-DOJMAIL SPAM Mailbox SOP
05-US-CERT Portal Advisories SOP
06-[redacted] SOP
07-Blocklist SOP
08-New Personnel SOP
09-EOUSA Daily Incident Report SOP
10-On-Call Incident Response SOP
11-Forensic Processing
12-Cyber Threat Analysis Team SOP
13-Vulnerability Patch Requirements Alert SOP
14-SCIF SOP
15-Network Tap SOP
SCIF Secret Monitoring SOP (Redacted)
SCIF Top Secret Monitoring SOP (Redacted)
DOJ Computer System Incident Response Plan
DoS Cyber Threat Handbook
Incident Reporting Handbook
Tactical Plan
IT Security Program Management Plan

THE JUSTICE MANAGEMENT DIVISION'S RESPONSE

U.S. Department of Justice

SEP 07 2011 *Washington, DC 20530*

MEMORANDUM FOR RAYMOND J. BEAUDET
ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL

FROM: Eric R. Olson
Acting Chief Information Officer

SUBJECT: Response to Audit Report of the Justice Security Operations Center's Capabilities and Coordination

This responds to the Draft Audit Report of the Justice Security Operations Center's Capabilities and Coordination and concurs with the recommendations.

We would like to thank the Inspector General's office for acknowledging that the Department has made significant progress in the area of IT security including the development of the JSOC in 2007. The JSOC has continually worked to improve and mature the capabilities at the enterprise level across all components, and this year expanded to 24x7 operations. While the JSOC has many processes and procedures currently in place to provide effective monitoring, actions are underway to further clarify and remove any conflicts between internal documents regarding component reporting requirements.

Additionally, the JSOC is refining existing incident ticketing processing to include integration of component processes. The JSOC has already enhanced the Incident Reporting Handbook and the Quality Assurance and Ticket Closure Standard Operating Procedure to address many of the recommendations identified in the report. Below is a summary of actions undertaken to address the reports' recommendations.

Recommendation # 1
Establish and document guidelines regarding the timeframe of incident reporting based on the risk assessment of US-CERT reporting requirements regarding incident detection for both components to JSOC and JSOC to US-CERT reporting.

DOJ Response
JMD concurs with this recommendation. JSOC has established and documented guidelines regarding the timeframe of incident reporting based on the risk assessment of US-CERT reporting requirements regarding incident detection for both components to JSOC and JSOC to US-CERT reporting.

JSOC policy regarding reporting timeframes was updated on July 20, 2011 within section 3.1 of *JSOC HB 11 – Incident Reporting Handbook* (available upon request for review in the JSOC) and section 9.3 of the DOJ Incident Response Plan (IRP) in accordance with the OIG recommendation. Reporting guidelines were briefed to component security personnel at the July CDO meeting on July 21, 2011. The DOJ IRP is available on the DOJ intranet at the JSOC homepage (http://dojnet.doj.gov/jmd/irm/itsecurity/jsoc-cyber-defense.php).

Recommendation # 2
Perform and document a risk assessment on each category risk to determine acceptable timeframe for closure of an incident.

DOJ Response
JMD concurs with this recommendation. The JSOC will perform and document a risk assessment on each category risk to determine acceptable timeframe for closure of an incident. Risk assessment will be completed by 9/30/11. This information will be documented in *JSOC HB 11 – Incident Reporting Handbook.*

Recommendation # 3
Document oversight and follow-up of open incident tickets at least weekly for all US-CERT-reportable incidents and for incidents under investigation.

DOJ Response
JMD concurs with this recommendation. The JSOC has documented oversight and follow-up of open incident tickets at least weekly for all US-CERT-reportable incidents and for incidents under investigation. JSOC policy regarding follow-up of open incidents was updated on July 20, 2011 within section 3.1.1.1.2 of *JSOC SOP 10 – Quality Assurance and Ticket Closure* (available upon request for review in the JSOC).

Recommendation # 4
Document reasons for ticket category changes within Remedy.

DOJ Response
JMD concurs with this recommendation. The JSOC has updated the policy/procedure that requires JSOC analysts to record a work log entry for any category change within a Remedy ticket. This requirement was updated on July 20, 2011 as an integrity check within section 3.1.1.2.1.3.1 *JSOC SOP 10 – Quality Assurance and Ticket Closure* (available upon request for review in the JSOC).

Recommendation # 5
Provide additional guidance regarding Remedy ticket classification to JSOC analysts and components to ensure awareness of appropriate category placement.

DOJ Response
JMD concurs with this recommendation. The JSOC has provided additional guidance regarding Remedy ticket classification to JSOC analysts and components to ensure awareness of appropriate category placement. New procedures were implemented during the audit and the JSOC policy was updated on July 20, 2011 within section 3.1.1.2 JSOC *SOP 10 – Quality Assurance and Ticket Closure* (available upon request for review in the JSOC) in accordance with the OIG recommendation. Incident categorization guidance was briefed to component security personnel at the July CDO meeting on July 21, 2011. Improvement between the 2 OIG ticket sample reviews indicates a successful implementation of the new policy guidance.

Recommendation # 6
Document policies regarding required information for closure.

DOJ Response
JMD concurs with this recommendation. The JSOC has documented policies regarding required information for analyst closure. The JSOC policy was updated on July 20, 2011 within section 3.2 *JSOC SOP 10 – Quality Assurance and Ticket Closure* (available upon request for review in the JSOC).

Recommendation # 7
Ensure Remedy tickets include sufficient documentation for closure.

DOJ Response
JMD concurs with this recommendation. The JSOC has documented policies to ensure Remedy tickets include sufficient documentation for closure. The JSOC implemented an integrity check on July 20, 2011 within section 3.2 *JSOC SOP 10 – Quality Assurance and Ticket Closure* (available upon request for review in the JSOC) in accordance with the OIG recommendation.

Recommendation # 8
Provide additional written requirements to both JSOC analysts and components regarding reporting timeframes and ensure reporting is based on requirements established.

DOJ Response
JMD concurs with this recommendation. The JSOC has provided additional written requirements to both JSOC analysts and components regarding reporting timeframes and has corrected the conflict in the 2 guidance documents. JSOC policy regarding reporting timeframes was updated on July 20, 2011 within section 3.1 *JSOC HB 11 – Incident Reporting Handbook* (available upon request for review in the JSOC) and section 9.3 of DOJ Incident Response Plan (IRP) in accordance with the OIG recommendation. Reporting guidelines were briefed to component security personnel at the July CDO meeting on July 21, 2011. The DOJ IRP is available on the DOJ intranet at the JSOC homepage http://dojnet.doj.gov/jmd/irm/itsecurity/jsoc-cyber-defense.php).

Recommendation # 9
Improve monitoring through JSOC's Quality Assurance Program and documentation that supports oversight of the Remedy Ticket lifecycle; including categorization, follow up and resolution.

DOJ Response
JMD concurs with this recommendation. The JSOC has formally documented and implemented procedures to improve monitoring through JSOC's Quality Assurance Program and documentation that supports oversight of the Remedy Ticket lifecycle; including categorization, follow up and resolution. The JSOC implemented a series of integrity checks on July 20, 2011 within section 3.1.1 *JSOC SOP 10 - Quality Assurance and Ticket Closure* (available upon request for review in the JSOC).

Recommendation # 10
Document policies and procedures for post-resolution modifications.

DOJ Response
JMD concurs with this recommendation. The JSOC has documented policies and procedures for post-resolution modifications. The JSOC implemented a series of integrity checks on July 20, 2011 within section 3.2.1.4.6 *JSOC SOP 10 - Quality Assurance and Ticket Closure* (available upon request for review in the JSOC) in accordance with the OIG recommendation. In addition, the JSOC implemented a programmatic hard-coded system change on July 26, 2011 in Remedy to lock the notes field post-resolution and enable auditing of the workflow logs.

Recommendation # 11
Ensure that any modifications that occur post-resolution are easily identifiable and that non auditable modifications are restricted from being modified post-resolution.

DOJ Response
JMD concurs with this recommendation. The JSOC has implemented new policy, procedures and technical controls to ensure that any modifications that occur post-resolution are easily identifiable and that non auditable modifications are restricted from being modified post-resolution. The JSOC implemented a series of integrity checks on July 20, 2011 within section 3.2.1.4.6 *JSOC SOP 10 - Quality Assurance and Ticket Closure* (available upon request for review in the JSOC) in accordance with the OIG recommendation. In addition, the JSOC implemented a programmatic hard-coded system change on July 26, 2011 in Remedy to lock the notes field post-resolution and enable auditing of the workflow logs.

Recommendation # 12
Define, in detail, "widespread" incidents for all malicious incidents at DOJ.

DOJ Response
JMD concurs with this recommendation. The JSOC has implemented policy to define, in detail, "widespread" incidents for all malicious incidents at DOJ.

The JSOC policy was updated on July 20, 2011 within section 4.1 *JSOC HB 11 – Incident Reporting Handbook* (available upon request for review in the JSOC).

Recommendation # 13
Document detailed methodology of tracking "widespread" incidents in Remedy and track these incidents in Remedy to report to US-CERT.

DOJ Response
JMD concurs with this recommendation. The JSOC has documented detailed methodology of tracking "widespread" incidents in Remedy and is able track these incidents in Remedy to report to US-CERT. The JSOC policy was updated on July 20, 2011 within sections 4.2 and 4.3 *JSOC HB 11 – Incident Reporting Handbook* (available upon request for review in the JSOC).

Recommendation # 14
Finalize all policies and update policies to reflect current operations including defining JSOC reportable sub-categories on all applicable documents and the inclusion of the "Closer" role.

DOJ Response
JMD concurs with this recommendation. The JSOC has finalized all policies and updated policies to reflect current operations including defining JSOC reportable sub-categories on all applicable documents and the inclusion of the "Closer" role. JSOC policy regarding reportable sub-categories was updated on July 20, 2011 within section 3.1 *JSOC HB 11 – Incident Reporting Handbook* (available upon request for review in the JSOC) and section 9.3 of the DOJ Incident Response Plan (IRP) in accordance with the OIG recommendation. The JSOC implemented a series of integrity checks to ensure proper ticket closure on July 20, 2011 within section 3.2 *JSOC SOP 10 - Quality Assurance and Ticket Closure* (available upon request for review in the JSOC).

Recommendation # 15
Ensure JSOC analysts and components are aware of updates to policies.

DOJ Response
JMD concurs with this recommendation. The JSOC participates in the quarterly Information Technology Security Governance Council (ITSCG) meetings to discuss changes to JSOC requirements, processes, and policies at the component CIO level, and will be briefing the Executive Officers during the September 2011 meeting. JSOC Management reviews all policy changes at weekly team meetings and with Components at monthly CDO and ITSC meetings. Components are also notified of pending changes and threats via the JSOC Security Advisories, JCON Broadcasts, and monthly newsletters. All notifications are also available on the DOJ intranet at the JSOC homepage (http://dojnet.doj.gov/jmd/irm/itsecurity/jsoc-cyber-defense.php).

Recommendation # 16
Obtain system feeds from all DOJ components to JSOC for review and trending purposes.

DOJ Response
JMD concurs with this recommendation. The JSOC is currently working with component security personnel to obtain system feeds from all DOJ components to JSOC for review and trending purposes. JSOC is currently upgrading major tools within its environment to accommodate all the additional feeds requested from Components and expects the upgrade to be completed by October 1, 2011. JSOC will provide a new Component feed schedule once the new tools are fully implemented to close this finding.

Recommendation # 17
Determine and evaluate component needs and areas for improved JSOC support services.

DOJ Response
JMD concurs with this recommendation. The JSOC is continually working to determine and evaluate component needs and areas for improved JSOC support services. The JSOC will continue to host monthly Cyber Defense Operations (CDO) and present at the monthly IT Security Committee (ITSC) meetings. The JSOC is also a participant in the CIO Council and ITSGC governance meetings where department/component priorities are developed and agreed upon. JSOC tailors service offerings to these initiatives. These meetings allow JSOC and IT Security POCs from components to discuss new JSOC service offerings, provide feedback to proposed changes or enhancements and make suggestions regarding key security issues throughout the Department. Additionally, the JSOC will update the existing services brochure and distribute to all components at the meetings.

Recommendation # 18
Continue and improve providing information to components regarding all JSOC services and responsibilities.

DOJ Response
JMD concurs with this recommendation. The JSOC will strive to continue and improve providing information to components regarding all JSOC services and responsibilities. The JSOC participates in the quarterly Information Technology Security Governance Council (ITSCG) and CIO Council meetings to discuss service offerings to the component CIO's, and will be briefing the Executive Officers during the September meeting on available services, responsibilities and data feed requirements.

The JSOC will continue to host monthly Cyber Defense Operations (CDO) and present at the monthly IT Security Committee (ITSC) meeting. These meetings allow JSOC and IT Security POCs from Components to discuss new JSOC service offerings and key security issues throughout the Department. JSOC will continue to produce Weekly Cyber Briefings; Vulnerability Patch Requirement (VPR) Alerts; Security Advisories; End of Month Reports; User-based informational newsletters, quarterly Classified Briefings; as well as, the annual CyberFest's Brown Bag Series.

JSOC management encourages Component tours of its facilities, makes onsite Component visits, provides onsite Engineering SMEs support to Components, and is a major contributor in the success of the DOJ Cyber Security Conference. All notifications are also available on the DOJ intranet at the JSOC homepage (http://dojnet.doj.gov/jmd/irm/itsecurity/jsoc-cyber-defense.php).

Recommendation # 19
Review and update JSOC policies to clarify potentially conflicting information regarding reporting of Category 6 incidents.

DOJ Response
JMD concurs with this recommendation. The JSOC reviewed and updated JSOC policies to clarify conflicting information regarding reporting of Category 6 incidents. JSOC policy regarding category 6 incidents was updated on July 20, 2011 within section 3.1 JSOC *HB 11 – Incident Reporting Handbook* (available upon request for review in the JSOC) and section 9.3 of the DOJ Incident Response Plan (IRP). The DOJ IRP is available on the DOJ intranet at the JSOC homepage (http://dojnet.doj.gov/jmd/irm/itsecurity/jsoc-cyber-defense.php).

Recommendation # 20

Determine a policy regarding appropriate periodic reporting for Category 6 incidents received from components.

DOJ Response

JMD concurs with this recommendation. The JSOC has finalized the policy regarding appropriate periodic reporting for Category 6 incidents received from components. JSOC policy regarding Category 6 incidents was updated on July 20, 2011 within section 3.1 JSOC *HB 11 – Incident Reporting Handbook* (available upon request for review in the JSOC) and section 9.3 of the DOJ Incident Response Plan (IRP) in accordance with the OIG recommendation. JSOC has updated CAT 6 reporting time frame language of the JSOC Incident Categories document to match the DOJ IRP which is available on the DOJ intranet at the JSOC homepage (http://dojnet.doj.gov/jmd/irm/itsecurity/jsoc-cyber-defense.php).

If you have any questions or need additional information, please contact Holly Ridgeway of the Information Technology Security Staff at (202) 616-0653 or by email at Holly.Ridgeway@usdoj.gov.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to JMD. JMD's response is incorporated in Appendix IV of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendation Number:

1. **Resolved.** JMD concurred with our recommendation to establish and document guidelines regarding the timeframe of incident reporting based on the risk assessment of US-CERT reporting requirements regarding incident detection for both components to JSOC and JSOC to US-CERT reporting. JMD stated in its response that JSOC has established and documented guidelines regarding the timeframe of incident reporting based on the risk assessment of US-CERT reporting requirements regarding incident detection for both components to JSOC and JSOC to US-CERT reporting.

   This recommendation can be closed when we receive evidence of the risk assessment of US-CERT reporting requirements, guidelines established by JSOC regarding the timeframe based on a risk assessment of US-CERT reporting requirements as updated in *JSOC HB 11 – Incident Reporting Handbook* and the DOJ Incident Response Plan, and evidence of component briefing of reporting guidelines.

2. **Resolved.** JMD concurred with our recommendation to perform and document a risk assessment on each category risk to determine acceptable timeframe for closure of an incident. JMD stated in its response that JSOC will perform and document a risk assessment on each category risk to determine acceptable timeframe for closure of an incident and document it in the *JSOC HB 11 – Incident Reporting Handbook*.

   This recommendation can be closed when we receive the updated *JSOC HB 11 – Incident Reporting Handbook* documenting the risk assessment on each category risk.

3. **Resolved.** JMD concurred with our recommendation to document oversight and follow-up of open incident tickets at least weekly for all

US-CERT reportable incidents and for incidents under investigation. JMD stated that JSOC has documented oversight and follow-up of open incident tickets at least weekly for all US-CERT reportable incidents and for incidents under investigation. JSOC also updated the *JSOC SOP 10 – Quality Assurance and Ticket Closure* regarding follow-up of open incidents.

This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* documenting the update of follow-up of open incidents.

4. **Resolved.** JMD concurred with our recommendation to document reasons for ticket category changes within Remedy. JMD stated that JSOC has updated the *JSOC SOP 10 – Quality Assurance and Ticket Closure* policy that requires JSOC analysts to record a work log entry for any category change within a Remedy ticket as an integrity check.

   This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* documenting the requirement for JSOC analysts to record a work log entry for any category change within a Remedy ticket as an integrity check.

5. **Resolved.** JMD concurred with our recommendation to provide additional guidance regarding Remedy ticket classification to JSOC analysts and components to ensure awareness of appropriate category placement. JMD stated that JSOC has provided additional guidance regarding Remedy Ticket classification to JSOC analysts and components to ensure awareness of appropriate category placement. New procedures were updated in *JSOC SOP 10 – Quality Assurance and Ticket Closure*. Incident categorization guidance was briefed to component security personnel at the July 2011 Cyber Defense Operations meeting.

   This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* documenting additional guidance regarding Remedy Ticket classification to JSOC analysts and components to ensure awareness of appropriate category placement.

6. **Resolved.** JMD concurred with our recommendation to document policies regarding required information for closure. JMD stated that JSOC has documented policies regarding required information for analyst closure in *JSOC SOP 10 – Quality Assurance and Ticket Closure.*

   This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* documenting required information for analyst closure.

7. **Resolved.** JMD concurred with our recommendation to ensure Remedy tickets include sufficient documentation for closure. JMD stated that JSOC has documented policies regarding sufficient documentation for closure. The JSOC implemented an integrity check in *JSOC SOP 10 - Quality Assurance and Ticket*.

   This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* implementing an integrity check regarding sufficient documentation for closure.

8. **Resolved.** JMD concurred with our recommendation to provide additional written requirements to both JSOC analysts and components regarding reporting timeframes and ensure reporting is based on requirements established. JMD stated that JSOC has provided additional written requirements to analysts and components regarding reporting timeframes and has corrected the conflict in the two guidance documents. JSOC policy regarding reporting timeframes was updated in *JSOC HB 11 – Incident Reporting Handbook* and the DOJ Incident Reporting Handbook. Reporting guidelines were briefed to component security personnel at the July 2011 Cyber Defense Operations meeting.

   This recommendation can be closed when we receive the updated *JSOC HB 11 – Incident Reporting Handbook,* the DOJ Incident Reporting Handbook, and evidence of the corrected conflict in the two guidance documents regarding reporting timeframes based on requirements established.

9. **Resolved.** JMD concurred with our recommendation to improve monitoring through JSOC's Quality Assurance Program and documentation that supports oversight of the Remedy Ticket lifecycle; including categorization, follow up, and resolution. JMD stated that

JSOC has formally documented and implemented procedures to improve monitoring through JSOC's Quality Assurance Program and documentation that supports oversight of the Remedy Ticket lifecycle; including categorization, follow up, and resolution. JSOC implemented a series of integrity checks in the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure*.

This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* documenting the implemented series of integrity checks to improve oversight of the Remedy Ticket lifecycle and monitoring through JSOC's Quality Assurance Program.

10. **Resolved.** JMD concurred with our recommendation to document policies and procedures for post-resolution modifications. JMD stated that JSOC has documented policies and procedures for post-resolution modifications. JSOC has implemented a series of integrity checks documented in *JSOC SOP 10 – Quality Assurance and Ticket Closure*. In addition, JSOC has implemented a programmatic hard-coded system change in Remedy to lock the notes field post-resolution and enable auditing of the workflow logs.

    This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* documenting the implemented series of integrity checks regarding post-resolution modification, and are provided evidence that the Remedy system locks the notes field post-resolution.

11. **Resolved.** JMD concurred with our recommendation to ensure that any modifications that occur post-resolution are easily identifiable and that non auditable modifications are restricted from being modified post-resolution. JMD stated that JSOC has implemented new policy, procedures and technical controls to ensure that modifications that occur post-resolution are easily identifiable and that non auditable modifications are restricted from being modified post-resolution. JSOC implemented a series of integrity checks documented in *JSOC SOP 10 – Quality Assurance and Ticket Closure*. JSOC also implemented a programmatic hard-coded system change to Remedy to lock the notes field post-resolution and enable auditing of the workflow logs.

    This recommendation can be closed when we receive the updated *JSOC SOP 10 – Quality Assurance and Ticket Closure* documenting the implemented series of integrity checks to ensure that modifications

that occur post-resolution are easily identifiable and that non auditable modifications are restricted from being modified post-resolution, and are provided evidence that the Remedy system locks the notes field post-resolution.

12. **Resolved.** JMD concurred with our recommendation to define, in detail, "widespread" incidents for all malicious incidents at DOJ. JMD stated that JSOC has updated the *JSOC HB 11 – Incident Reporting Handbook* to define, in detail, "widespread" incidents for all malicious incidents at DOJ.

    This recommendation can be closed when we receive the updated *JSOC HB 11 – Incident Reporting Handbook* documenting the definition, in detail, of "widespread" incidents for all malicious incidents at DOJ.

13. **Resolved.** JMD concurred with our recommendation to document detailed methodology of tracking "widespread" incidents in Remedy and track these incidents in Remedy to report to US-CERT. JMD stated that JSOC has documented detailed methodology of tracking "widespread" incidents in Remedy in the *JSOC HB 11 – Incident Reporting Handbook* and is able to track these incidents in Remedy to report to US-CERT.

    This recommendation can be closed when we receive the updated *JSOC HB 11 – Incident Reporting Handbook* documenting the tracking of "widespread" incidents in Remedy to report to US-CERT.

14. **Resolved.** JMD concurred with our recommendation to finalize all policies and update policies to reflect current operations including JSOC reportable sub-categories on all applicable documents and the inclusion of the "Closer" role. JMD stated that JSOC has finalized all policies and updated policies to reflect current operations including defining JSOC reportable sub-categories on all applicable documents and the inclusion of the "Closer" role. JSOC updated *JSOC HB 11 – Incident Reporting Handbook* and the DOJ Incident Response Plan to include policy regarding reportable sub-categories. JSOC also implemented a series of integrity checks to ensure proper ticket closure in *JSOC SOP 10 – Quality Assurance and Ticket Closure*.

    This recommendation can be closed when we receive the *JSOC HB 11 – Incident Reporting Handbook* and the DOJ Incident Response Plan documenting reportable sub-categories, and *JSOC SOP 10 – Quality*

Assurance and Ticket Closure documenting the implementation of a series of integrity checks to ensure proper ticket closure.

15. **Resolved.** JMD concurred with our recommendation to ensure JSOC analysts and components are aware of updates to policies. JMD stated that JSOC participates regularly in quarterly Information Technology Security Governance Council meetings to discuss changes to JSOC requirements, processes, and policies at the component CIO level, and will brief Executive Officers during the September 2011 meeting. JSOC management reviews all policy changes at weekly team meetings and with components at weekly Cyber Defense Operations and Information Technology Security Committee meetings. Additionally, components are notified of pending changes and threats via the JSOC Security Advisories, JCON Broadcasts, and monthly newsletters.

    This recommendation can be closed with evidence of the briefing to Executive Officers regarding changes to JSOC requirements, processes, and policies.

16. **Resolved.** JMD concurred with our recommendations to obtain system feeds from all DOJ components to JSOC for review and trending purposes. JMD stated that JSOC is working with component security personnel to obtain system feeds from all DOJ components for review and trending purposes. JSOC is currently upgrading major tools within its environment to accommodate all the additional feeds requested from components and expects the upgrade to be completed by October 2011.

    This recommendation can be closed when we receive evidence that JSOC receives all requested component feeds.

17. **Resolved.** JMD concurred with our recommendations to determine and evaluate component needs and areas for improved JSOC support services. JMD stated that JSOC is continually working to determine and evaluate component needs and areas for improved JSOC support services. JSOC will continue to host Cyber Defense Operations meetings and present at monthly Information Technology Security Committee meetings. JSOC is also a participant in the CIO Council and Information Technology Security Governance Council meetings where Department and component priorities are developed and agreed upon. JSOC tailors service offerings to these initiatives. These meetings allow JSOC and component IT security points of contact to

discuss new JSOC service offerings, provide feedback to proposed changes or enhancements, and make suggestions regarding key security issues throughout the Department. JSOC will also update the existing services brochure and distribute to all components at meetings.

This recommendation can be closed when we receive the updated existing services brochure and evidence of component and JSOC discussions regarding JSOC services.

18. **Resolved.** JMD concurred with our recommendation to continue and improve providing information to components regarding all JSOC services and responsibilities. JMD stated that JSOC will strive to continue and improve providing information to components regarding all JSOC services and responsibilities. JSOC participates in the quarterly Information Technology Security Governance Council and the CIO Council meetings to discuss service offerings to the component CIO's and will be briefing Executive Officers in September 2011 regarding available services, responsibilities and data feed requirements. JSOC will continue to host monthly Cyber Defense Operations meetings and present at the monthly Information Technology Security Committee meetings that allow JSOC and component IT security staff to discuss JSOC service offerings and key security issues throughout the Department. JSOC will continue to produce Weekly Cyber Briefings; Vulnerability Patch Requirement Alerts, Security Advisories, End of Month reports, user-based informational newsletters, quarterly classified briefings, as well as the annual CyberFest Brown Bag series.

    This recommendation can be closed when we receive evidence that JSOC briefed the Executive Officers regarding available services, responsibilities, and data feed requirements.

19. **Resolved.** JMD concurred with our recommendation to review and update JSOC policies to clarify potentially conflicting information regarding reporting of Category 6 incidents. JMD stated that JSOC reviewed and updated JSOC policies regarding Category 6 incidents. JSOC policy regarding Category 6 incident information was updated in *JSOC HB 11 – Incident Reporting Handbook* and the DOJ Incident Response Plan were updated regarding Category 6 incident information.

This recommendation can be closed when we receive *JSOC HB 11-Incident Reporting Handbook* and the DOJ Incident Response documenting the updated Category 6 incident information.

20. Resolved. JMD concurred with our recommendation to determine a policy regarding appropriate periodic reporting for Category 6 incidents received from components. JMD stated that JSOC finalized the policy regarding periodic reporting for Category 6 incidents and updated *JSOC HB 11 – Incident Reporting Handbook* and the DOJ Incident Response Plan. JSOC also updated the Category 6 reporting timeframe language of the JSOC Incident Categories document to match the DOJ Incident Response Plan.

This recommendation can be closed when we receive *JSOC HB 11-Incident Reporting Handbook* and the DOJ Incident Response Plan documenting the update for appropriate periodic reporting for Category 6 incidents.